Doctoral theses at NTNU, 2023:112

Grethe Østby

# Digital transformation of public security - developing triple-loop-learning artifacts to meet emerged information security incident response resilience and readiness challenges in public emergency organizations

Doctoral thesis

NTNU
Norwegian University of Science and Technology
Thesis for the Degree of Philosophiae Doctor
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of Science and Technology

Grethe Østby

# Digital transformation of public security - developing triple-loop-learning artifacts to meet emerged information security incident response resilience and readiness challenges in public emergency organizations

Thesis for the Degree of Philosophiae Doctor

Trondheim, April 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

**NTNU**
Norwegian University of Science and Technology

Thesis for the Degree of Philosophiae Doctor

Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology



ISBN 978-82-326-6051-3 (printed ver.)
ISBN 978-82-326-5292-1 (electronic ver.)
ISSN 1503-8181 (printed ver.)
ISSN 2703-8084 (online ver.)

Doctoral theses at NTNU, 2023:112

Printed by NTNU Grafisk senter

Til mor og far - for å gi meg klar beskjed om å ikke gi opp!
Til gode venner - for å lytte uten å behøve å lytte.
Til Marvin - fordi du begrenset meg; «når jeg ikke kan game etter klokka ti, da kan ikke du jobbe etter klokka ti», men også fordi du og jeg nå vet at det finnes muligheter. Nå skal vi klare oss.

Abstract

Studies have found that resilience and response capabilities in a cyber-attack are unfamiliar to organizations, and it is also found that not only the IT-personnel, but also the crisis management group and teams need socio-technical resilience and readiness to handle such attacks.

To overcome this resilience and readiness gap in the society and shortage of trained personnel to handle information security incidents, this project was established to suggest effective and efficient methods and tools and artifacts to train and work with information- and cyber security incident management in all organizations in general and particularly in public emergency organizations.

The Design Science Research in Information Security as a pragmatism philosophical perspective was chosen for this project to develop learning artifacts to close the resilience and readiness gap in public emergency organizations. The research was approached with a naive inductive approach, and the strategy has been to meet the challenges with multiple mixed methods, and several public emergency organizations have been invited to take part in the research. Mostly, the studies have been cross-sectional, but the student-exercise have been executed over a 3-year period (longitude). The collection of data was initially done explanatory and descriptive, but exploratory data collection was collected to discuss and validate the findings. To analyze the data, socio-technical root-cause-analysis, categorical analysis from descriptive data/results questionnaires and expected/not expected or yes/no questions (dichotomous descriptive data), and qualitative effect analysis from the variety of actions, were used.

In this thesis summary, several key concepts from the research project that have been developed and published in conference proceedings and journals are presented, together with analyzes of data from case-studies, training and exercises executed in the period of the research. Two publications and one report (appendix) present the current level of resilience and readiness in public emergency organizations, five of the publications and the appendix presents learning knowledge and learning frameworks, and four of the publications presents frameworks to learn from exercises.

The major findings of this project are that a preparation for exercises framework and how to build EXCON teams for full-scaled information- and cyber security exercises has received very little attentions in the research community, and also in regard to societal training for readiness and resilience experiencing a cyber-attack. It was also established that 1) triple-loop-learning and 2) scoping development of serious games for information- and information- and cyber security incident response, are both relevant and new approaches to information security management exercises. Fine-tuned coordinated learning activities to meet the timeline of a scenario, and triple-loop-learning activities for use in the exercises are of great importance, and a user-centric-approach is of importance to be able to implement the activities at the right level in the organization and to close the gap one step at the time. Finally, socio-technical learning activities have shown that 1) targeted exercise goals developed in the scenarios are met during the exercises, 2) socio-technical step-by-step improvement can be developed based on the level of escalation maturity, and 3) organizations can learn from training and exercises.

## Sammendrag

Studier har funnet at responsevner i et cyberangrep er et ukjent område for mange organisasjoner, og det er også funnet at ikke bare IT-personell, men også krisehåndteringsgrupper og øvrige team trenger sosioteknisk bevissthet om slik risiko, og ikke minst opplæring for å håndtere slike angrep.

For å overvinne samfunnsutfordringene med informasjonssikkerhet og mangelen på trent personell til å håndtere informasjonssikkerhetshendelser, ble dette prosjektet etablert for å utarbeide nødvendige og effektive metoder og verktøy for å best trene til og øve på håndtering av informasjons- og cybersikkerhetshendelser i alle organisasjoner generelt og i offentlige beredskapsorganisasjoner spesielt.

Design Science Research in Information Security som pragmatisk filosofisk perspektiv ble valgt for dette prosjektet for å utvikle læringsartefakter for å lukke motstands- og beredskapsgapet i offentlige beredskapsorganisasjoner. Det ble benyttet en naiv induktiv tilnærming til forskningen, og strategien var å møte utfordringene med flere ulike metoder, og flere offentlige beredskapsorganisasjoner har vært invitert til å ta del i forskningen. Studiene har for det meste vært tverrsnitts studier, men studentøvelsen ble gjennomført over en 3-års periode (longitudinell studie). Innsamlingen av data ble i utgangspunktet gjort forklarende og beskrivende, men utforskende datainnsamling ble benyttet for å diskutere og validere funnene. For å analysere dataene ble det brukt sosiotekniske rotårsaksanalyser, kategorisk analyse fra beskrivende data/resultatspørreskjemaer og forventet/ikke forventet eller ja/nei-spørsmål (dikotome deskriptive data), og kvalitativ effektanalyse fra aksjonsforskning.

I denne oppgaven presenteres flere sentrale konsepter for forskningsprosjektet, som er utviklet og publisert i vitenskapelige konferanser og tidsskrifter, sammen med analyser av data fra case-studier, opplæring, og øvelser utført i forskningsperioden. To publikasjoner og en rapport (vedlegg) presenterer dagens evne til motstand og beredskap i offentlige beredskapsorganisasjoner, fem av publikasjonene og rapporten presenterer kunnskap om læring og rammeverk for læring, og fire av publikasjonene presenterer rammeverk for å lære fra øvelser.

De viktigste funnene fra dette forskningsarbeidet er at forberedelse til øvelser og hvordan bygge spillstab-team for fullskala informasjons- og cybersikkerhetsøvelser er nytt i forsknings miljøet, og også nytt i forhold til samfunnsopplæring for beredskap og motstandsevne ved et cyberangrep. Forskningen tilsier også at 1) trippel-loop-learning og 2) utvikling av seriøse spill for informasjons- og cybersikkerhetshendelser, er både relevante og nye tilnærminger til ledelsesøvelser for informasjonssikkerhet. Finjusterte koordinerte læringsaktiviteter for å møte tidslinjen til et scenario, og triple-loop-læringsaktiviteter til bruk i øvelsene er av stor betydning, og en brukersentrisk tilnærming er viktig for å kunne gjennomføre aktivitetene på riktig nivå i organisasjonen og for å tette gap ett trinn av gangen. Et siste viktig funn er at sosiotekniske læringsaktiviteter har vist at 1) målrettede treningsmål utviklet i scenarioene oppfylles under øvelsene, 2) sosiotekniske trinnvise forbedringer kan utvikles basert på nivået på eskaleringsmodenhet, og 3) organisasjoner kan lære fra trening og øvelser.

Acknowledgements

In the spring of 2017, a couple of men from The Norwegian University of Science and Technology (NTNU) showed up in my office at the Norwegian civil defense national competence center, asking for collaboration. Rather quickly we contacted the Innlandet county governor head of emergency and asked if we could provide an information security table-top exercise for firstly the management group and operational emergency group at the county governor, but also secondly for the emergency council in the county. The county confirmed immediately, and soon we were in a planning process to execute the exercise. The exercise in the autumn of 2017 went well, and in the after-action review of the exercise, I suggested that the future should have been for me to do a master's in information security. Whereas professor Kowalski suggested that I should try for a PhD instead. Looking into different opportunities to financially cover the PhD, we ended up with financial support from the Innlandet county municipality (as part of the Norwegian Cyber Range innovation project) and the Innlandet hospital trust. I will be forever very grateful to Nils Kalstad, head of the Information security and technology department at NTNU, Stewart James Kowalski, Professor in Information security in the same department, the Innlandet county municipality, and the Innlandet hospital trust for giving me the possibility to do this PhD. And, as a helping hand both beforehand and during the PhD, the head of emergency at the Innlandet county general, Asbjørn Lund. Finally, with the granted permission from my employer, the Norwegian Directorate of Civil protection (DSB), the work could begin.

The work has consisted of several case-studies and exercises, and a lot of helping hands have made the work possible. Starting out with the case-studies, the first case-study was executed at the Innlandet hospital trust, supported by the head of the IT-department Roar Halvorsen and the CEO Alice Beate Andersgaard. A great thanks to all the participants in the case-study. The second case-study was executed at Gjøvik municipality, supported by the CEO Magnus Mathiesen and head of administration Marit Lium Dahlborg. A great thanks to the participants in that study also. The final case-study was executed in Østre Toten municipality, supported by CEO Ole Magnus Stensrud and Major Bror Helgestad. In total 28 participants answered the questionnaire and 9 participated in-depth interviews in this special case-study on how the municipality handled the massive cyber-attack they had to cope with in January 2021. Thanks to everyone participating – the results are of great interest for students and researchers, other municipalities, and other organizations.

Next, the work has included several exercises, either as a participant or in the lead. Firstly, my main supervisor Stewart James Kowalski gave me the opportunity to participate in a team (with young enthusiastic – I would call them boys) in the Atlantic Council's 9/12 Cyber security challenge, and thereafter as a coach one year, before finally the last two years as a judge.

Secondly, we run a table-top exercise for the IT-management-group at NTNU, and I would like to thank the head of the IT-management-group, Håkon Alstad, and moreover, the head of the EXCON-team for the exercise, Gaute Wangen, for making the exercise possible. Thanks to the IT-management group for participating, and thanks to all participants in the EXCON-team playing "the rest of the world".

Thirdly, Professor Kowalski initiated for me to administrate a Megagame which we arranged during the Security-festival in Lillehammer in 2019, and I would like to thank stonepaperscissors.com for providing the scenario and set-up, students from our department and from the Megagame environment in Oslo for stepping up as game-masters, and finally to all students from our department and from the Game technology and simulation department at Innlandet college, for participating.

Closer to Christmas 2019 we got an invitation from the Norwegian Directorate for Civil Protection (DSB) to participate in the national exercise Digital2020, and after Nils Kalstad and I met up with DSB in Tønsberg, I ended up participating in the group who developed the scenarios for those who would not have the possibility to attend the exercise itself. The group consisted of members from DSB, The Norwegian National Security authority (NSM), The Norwegian Digitalization directorate, The Norwegian center for information security (NorSIS), and me from NTNU. It was an inspiring period, and a good positive group to work within. A special thanks to Anders Gundersen and Helen Knutsen from DSB for running and administrating the work. We ended up with developing ovelse.no, a platform with discussion exercises based on 12 different known information security scenarios. The platform was developed at the Norwegian Cyber Range, and I will pay my thanks to Espen Torseth who led the system-implementation process of the platform.

Hit by the Covid19 pandemic in the midst of the PhD-journey, further exercises seemed unlikely for a period of time, but we did however manage to run a test-exercise at the cyber-range with students playing the participants, with an EXCON-team run by administrative personnel from our department, media personnel from NTNU communications department, personnel from the Innlandet county governor, and technical personnel and red-team personnel from our department. I am thankful to my co-supervisor Basel Katt, who was the head of the exercise, that my input to not just test the systems, but also to adapt and test how an EXCON-team should be set up for these types of exercises were executed.

Despite the Covid19 situation, I have been able to run digital information security management discussion exercises for the students in the IMT-4115 Introduction to information security management course. In this regard, I would like to pay special thanks to my learning assistants 1) in 2020: John Andre Seem, 2) in 2021: Job Nestor Bahner and Malene Vassenden, and finally in 3) 2022: Vilde Nylund Johnsen and Karianne Kjønås. Lucky are the employers who will get the chance to work with you!

In June 2022 we were finally (after the long period of Covid19) able to run an “on-campus” policy exercise for the partner group in the Center for Cyber and Information Security (CCIS), and I would like to thank Nils Kalstad for the opportunity to write the scenario and involve participants in this special type of policy-consideration exercise we created.

I am also very thankful to my co-supervisor Basel Katt (internal lead) and the heads of the exercise Morris (a security sectorial exercise within the University sector), Made Ziius, Ingrid Moen and Tor Gjerde at The Norwegian Agency for Shared Services in Education and Research (SIKT) for being able to participate in the exercise, and for being able to collect research data related to the training in the exercise.

In the autumn of 2022, we finally also got the chance to run a full-scaled information-security exercise with Akershus University hospital trust (Ahus) and Sykehuspartner, initiated by Hilde Alstad and Janne Pedersen from Ahus, and I am forever grateful to the management group at Ahus and the information security personnel at Sykehuspartner for participating in the exercise. Thanks also to the EXCON-team, who consisted of students and staff from our department playing media, technical experts, national authorities, and red-team, and a special thanks to Kåre Magne Stennes and Ruth-Ann Gullbekk from Ahus, and Tom Jensen from Sykehuspartner, playing the internal roles relevant for the organizations.

In November 2022, we got (on extremely short notice) the chance to execute an exercise for the management group at Kripos. And sometimes I think that I live in the best country in the world, as when I started to call around to get help for the exercise the "dugnad"-spirit of Norway emerged. Johan Martin Welhaven at Innlandet police district took the time to talk to me and guide me the way, and step-by-step I got in contact with Odin Heitmann in Kripos who took on the job to be the EXCON-leader, the IT-department at Kripos led by Lasse Gråberg, and justiceCERT by Gjermund Marquardsen and Glenn Gulliot. Through Else Marie Næss Starum and Svein Rune Enger I got in contact with Helle Holtlien from the Innlandet police district, who could play both police and prosecuting authority. To play the media-team, I internally got help from Maren Sophie Basset (master-student) and Lars Erik Pedersen, and externally from Hanne Stine Kind at NorSIS (who amongst other things has experience as a media counselor from the Police). Why do I mention everybody in this specific exercise? Because – against all odds – we made it!

A special thanks also to all my co-authors, Lars Berg, Mazaher Kianpour, Kieren Nicolas Lowell, Muhammad Mudassar Yamin, Bilal AlSabbagh, and therein of course also my co-supervisor Basel Katt and my main supervisor Stewart James Kowalski. In addition, I would like to thank for the opportunity to support students in their work and scientific publications, that is, Alexander Daniel Forfot and Philip Johannes Brugmans Nyblom.

Thank you also to the two master-students which collected the topics I had written and suggested relevant for my research project, Johan Olav Valdre Huseby and Bjørn Emil Selebø – your work is still relevant, and we are in the process of publishing collections especially from Bjørn Emil's work.

Finally, I would like to pay my thanks to Guro Wang Øverli at the NTNU communications department. Both for encouraging her staff to participate in the exercises, but also for the positive attitude and willingness to "spread the word" about our research to relevant media, and thereby for me to be able to talk about what we do to a broader audience.

Someone once told me that I have a lot of good helpers, and by writing this acknowledgement section I must agree to the statement. At the same time, I would like to make a call-out that this is what it is all about. To meet the increased information- and cybersecurity threat, we must help each other to raise the knowledge, skills, and competence necessary in the society today. In this regard, I would like to thank Professor Kowalski for his ever presence to raise focus on both social and technical aspects of information security, and moreover the importance of transactional research within social sciences which are needed in information security.

I suggest we should keep up giving a helping hand, we do after all have to depend on each other when we must raise to the information security occasions. Maybe we would learn something in the process as well?

Thanks!

Index


1 Introduction 23
1.1 Research problems 23
1.2 Research strategy 24
1.3 Objectives: Research goals and questions 26
1.4 Thesis summary overview 28
2 Research Methodology 31
2.1 Research philosophy 31
2.2 Research approach 35
2.3 Methodological choice and scope 36
2.4 Time horizon 39
2.5 Research strategies and research data sampling 39
2.6 Data analysis 42
2.6.1 Socio-technical root-cause-analysis 42
2.6.2 Descriptive categorical data analysis 43
2.6.3 Thematic exploratory analysis and participatory action research (qualitative analysis) 43
2.7 Ethical academically and societal considerations 44
2.8 Summary 45
3 Discussion results 47
3.1 Case studies crisis management 47
3.1.1 Cyber-attacks as separate risk and vulnerability assessment 50
3.1.2 Information requirements 51
3.1.3 ICT Incident Management and Recovery Team 52
3.1.4 Alert/notification team - sensitive personal data for sale on dark web 53
3.1.5 Internal communication - crack in the crisis line (?) 54
3.1.6 Training and exercises 55
3.2 Preparing for exercises as activity 56
3.3 Arranging and participating in games and executing exercises 63
3.3.1 Student exercises and participation in games 64
3.3.2 Exercises for organizations 67
4 Rigor and relevance 71
4.1 Frameworks of learning knowledge and learning frameworks 71
4.2 Review of literature on information security management in public organizations 74
4.2.1 Relevant research from exercises in public organizations 76

4.2.2 Relevant research from exercises in other sectors 76
4.2.3 Variety of exercises from the literature search 77
4.2.4 Learning activities 77
4.3 Summary 77
5 Concluding remarks and ongoing and future research directions 79
6 Epilog (see English below) 83
7 Epilogue English 85
8 References 87
9 Publications 95

List of figures


| Figure | |
|---|---|
| Fig. 1. | Public organizations capabilities to cope with crises and digital events |
| Fig. 2. | Chapter overview |
| Fig. 3. | The research 'onion' (Saunders et al., 2012) |
| Fig. 4. | Design research methodology in information systems (modified) (G. R. Karokola, 2012) |
| Fig. 5 | Socio-technical approach (Kowalski, 1994; Leavitt, 1965) |
| Fig. 6. | Naive inductivist approach (Chalmers, 1999; Kowalski, 1994) |
| Fig. 7. | The action research spiral (Kemmis et al., 2014) |
| Fig. 8. | Variety in views of maturity in reporting (Østby & Katt, 2019b) |
| Fig. 9. | Socio-technical root-cause analysis of the Identify and Protect phases of the NIST-framework (Østby & Kowalski, 2021). |
| Fig. 10. | Partial risk analysis (Østby & Kowalski, 2022c) |
| Fig. 11. | Need for information sharing during cyber-attacks - modified (Østby & Katt, 2019a) (publication 4) |
| Fig. 12. | Participants in tactical and operational teams - explained (Østby & Katt, 2019a) (publication 4) |
| Fig. 13. | Alert/notification team (Østby & Kowalski, 2022c) |
| Fig. 14. | New crisis management lines towards operational ICT team (Østby & Kowalski, 2022c) |
| Fig. 15. | User centric approach (Usability.gov, 2021) |
| Fig. 16. | Details from a socio-technical scenario |
| Fig. 17. | Maturity improvement process (Østby et al., 2020) (publication 2) |
| Fig. 18. | Different types of exercises (HSEEP, 2006) |
| Fig. 19. | Scoping development of serious games in information- and cyber security incident response in a master study course (Østby & Kowalski, 2022a) (publication 5) |
| Fig. 20. | Factors in the scenario the students scored as achieved (Østby & Kowalski, 2022b) (publication 3) |
| Fig. 21. | Pathways of and outcomes of single-, double- and triple-loop learning adapted from Medema (Medema et al., 2014; Østby & Kowalski, 2022b) (publication 3) |
| Fig. 22. | Targeted learning objectives met |
| Fig. 23. | Coordinated learning activities to meet the timeline of a scenario |
| Fig. 24. | Information systems research framework (Hevner et al., 2004) |
| Fig. 25. | Implement processes to learn action points (Østby et al., 2020) |
| Fig. 26. | Thematic rigor and relevance analysis |
| Fig. 27. | Contribution in the Norwegian Cyber Range project |
| Fig. 28. | Conclusions from thematic mapping of publications |
| Fig. 29. | Coordinated learning activities |

List of tables


| **Table** | |
|---|---|
| Table 1 | Comparison of research philosophies (Saunders et al., 2012) |
| Table 2 | Abduction, deduction, and induction approaches (Koingharara, 2022) |
| Table 3 | DSRIS as a pragmatic philosophical approach |
| Table 4 | Project, participants, and potential effects |
| Table 5 | Research questions, publications, and activities |
| Table 6 | Research methodology |
| Table 7 | ovelse.no users |
| Table 8 | Relevance of lectures beforehand exercises ICT-management team at NTNU (Østby & Kowalski, 2020) |
| Table 9 | Relevance of lectures beforehand exercises Ahus |
| Table 10 | Relevance of lectures beforehand exercise, student-exercise (Østby & Kowalski, 2022b) |
| Table 11 | Participation in and execution of exercises |
| Table 12 | Search string criterions |
| Table 13 | Results from search |

List of abbreviations

| Term | Description |
|---|---|
| NTNU | The Norwegian University of Science and Technology |
| PhD | Doctor of Philosophy |
| DSB | Direktoratet for samfunnssikkerhet og beredskap (The Norwegian Directorate for Civil Protection) |
| CCIS | Center for Cyber and Information Security |
| CEO | Chief Executive Officer |
| IT | Information technology |
| MM | Maturity modelling |
| EMM | Escalation maturity modelling |
| CMM | Capability maturity modelling |
| UCD | User centric design |
| EXCON | Exercise control |
| SI | Sykehuset Innlandet (Innlandet hospital trust) |
| Ahus | Akershus Universitetssykehus (Akershus University hospital trust) |
| NSM | Nasjonal sikkerhetsmyndighet (The Norwegian Security Authoroty) |
| NorSIS | Norsk senter for informasjonssikring (The Norwegian Center for Information Security) |
| SIKT | The Norwegian Agency for Shared Services in Education and Research |
| RQ | Research question |
| DSRIS | Design science research in information systems |
| NDA | Non-Disclosure Agreements |
| NSD | Norwegian Centre for Research data |
| PST | Primary search terms |
| SST | Secondary search terms |
| ST1 | Search string 1 |
| ST2 | Search string 2 |
| CIM | Crisis Information Management system |
| SIEM | Security Information Management and Event Management system |
| HSEEP | Homeland Security Exercise and Evaluation Program |
| NIST | US National Institute for Security and Technology |
| NICE | US National Initiative for Cybersecurity Education |
| OLC | Organizational Learning Culture |
| LO | Learning Organization |
| OL | Organizational Learning |
| SOC | Security Operation Center |
| CSIRT | Computer Security Incident Response Teams |
| ILAC | Institutional learning and change |
| NC3 | National cybercrime center |
| KS | Kommunesektorens interesseorganisasjon |
| CCIS | Center for Cyber and Information Security |
| CERT | Community Emergency Response Teams |
| UCD | User centric design |
| SWOT | Strengths Weaknesses Opportunities and Threats |

| | |
|---|---|
| CISO | Chief information security officer |
| ICT | Information and communication technology |
| ENISA | The European Union Agency for Cybersecurity |

List of publications and appendix

Publications

| | |
|---|---|
| Publication 1 | Østby, Grethe; Kowalski, Stewart James. (2021) A case study of a municipality phishing attack measures - towards a socio-technical incident management framework. *CEUR Workshop Proceedings. vol. 3016.* |
| Publication 2 | Østby, Grethe; Kowalski, Stewart James; Katt, Basel. (2020) Towards a Maturity Improvement Process – Systemically Closing the Socio-Technical Gap. *CEUR Workshop Proceedings. vol. 2789.* |
| Publication 3 | Østby, Grethe; Kowalski, Stewart James. (2022) ORGANIZATIONAL LEARNING WITH CRISES. *EDULEARN22 Proceedings.* Iated. |
| Publication 4 | Østby, Grethe; Katt, Basel. (2019) Cyber Crisis Management Roles – A Municipality Responsibility Case Study. *Information Technology in Disaster Risk Reduction.* Springer. |
| Publication 5 | Østby, Grethe; Kowalski, Stewart James. (2022) Introducing Serious Games as a Master Course in Information Security Management Programs: Moving Towards Socio-Technical Incident Response Learning. *Handbook of Research on Cross-Disciplinary Uses of Gamification in Organizations.* IGI Publishing. |
| Publication 6 | Østby, Grethe; Kowalski, Stewart James. (2020) Preparing for cyber crisis management exercises. *Augmented Cognition. Human Cognition and Behavior.* Springer. |
| Publication 7 | Østby, Grethe; Lovell, Kieren N.; Katt, Basel. (2020) EXCON Teams in Cyber Security Training. *2019 International Conference on Computational Science and Computational Intelligence (CSCI).* IEEE. |
| Publication 8 | Østby, Grethe; Berg, Lars; Kianpour, Mazaher; Katt, Basel; Kowalski, Stewart James. (2019) A Socio-Technical Framework to Improve cyber security training: A Work in Progress. *CEUR Workshop Proceedings. vol. 2398.* |

Appendix

| | |
|---|---|
| Appendix 1 | Hendelseshåndtering ved cyber-angrepet mot Østre Toten kommune https://www.ototen.no/aktuelt/rapport-etter-dataangrepet.15279.aspx |

# 1 Introduction

## 1.1 Research problems

Norway has become one of the most digitized countries in the world (European Parliament, 2017) and the drive for digitization in the Norwegian public sector continues.

> "Digitization shall promote a more efficient public sector, more value creation in the business sector and, not least, a simpler everyday life for most people." (The Norwegian Government, 2019)

As far back as in 2000, a Norwegian investigation found that the technological changes have made the society more vulnerable for failure in digital systems (The Norwegian justice and police department, 2000), but it was not until in 2019 a national strategy for digital security was introduced (The Norwegian Government, 2019a) together with several initiatives to meet the challenges (The Norwegian Government, 2019b). In 2019 the Norwegian Directorate for Civil Protection (DSB) also (first) introduced cyber-attack as a societal crisis scenario (DSB, 2019).

Two of the Office of the Auditor General of Norway's reports in 2019 and 2020 reported that capabilities of public emergency organizations to respond to cyber-attacks were 'strongly objectionable' (Riksrevisjonen, 2019, 2020) and also 'very serious' (Riksrevisjonen, 2020)[1]. In addition, according to the annual Cisco report from 2018, the number of CEO's that responded, 'lack of talent within information security as an obstacle', increased from 22 percent in 2015 to 27 percent in 2018 (Cisco, 2018). Consequently, not only are the capabilities of public emergency organizations low, but there is also a shortage of qualified individuals in the society.

In the crisis and incident handling report after the cyber-attack against Østre Toten municipality (Østby & Kowalski, 2022c), the findings confirmed that the municipality lacked adequate capabilities to deal with this type of cyber-attack. It also confirms the Auditor General of Norway's reports on how the response capabilities in a cyber-attack are unfamiliar to organizations. It was also found that not only the IT-personnel, but also the crisis management group and teams need socio-technical awareness of such risk, and training to handle a cyber-attack. Organizations as Østre Toten municipality's resilience and readiness to cope with cyber-attacks causing crises can be presented as in figure 1, where the municipality's digitization of services has increased faster than the capabilities to deal with the attacks, and an increased resilience and readiness gap from i.e., cyber-attacks would need to be addressed.

[1] The translations the Office of the Auditor General of Norway uses themselves are 'sterkt kritikkverdig' = 'strongly objectionable' and 'svært alvorlig' = 'very serious'

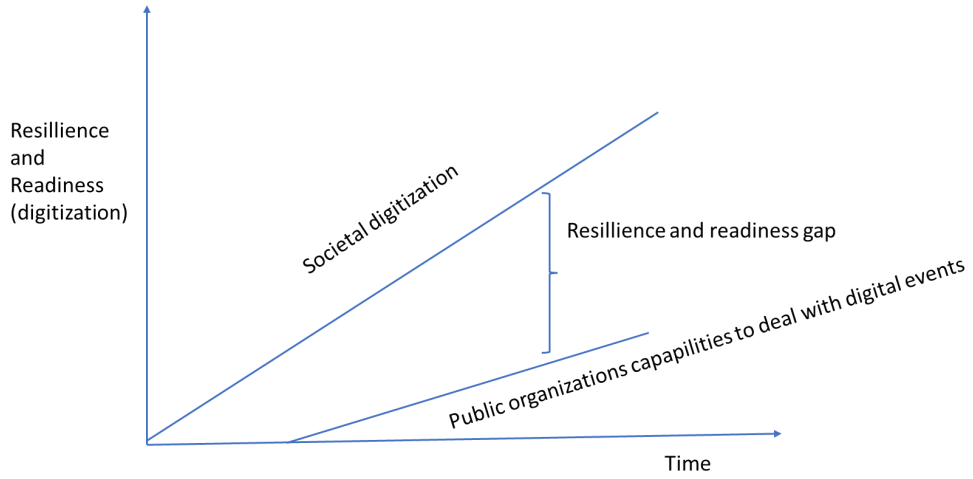



**Fig. 1.** Public organizations capabilities to cope with crises and digital events

To overcome this resilience and readiness gap in the society and shortage of trained personnel to handle information security incidents, this project was established to suggest effective and efficient methods and tools (artefacts) to train and work with information- and cyber security incident management in all organizations in general and particularly in public emergency organizations.

The public sector in Norway can be described as providers of services that a non-payer cannot be excluded from (such as building roads), services which benefit all of society rather than just the individual who uses the service. The primary focus of this research has been on the Norwegian public sector which is divided into public administration and public companies. Public administration is divided into local administration (municipalities and county administrational) and sectorial administration (military, police, civil defense, hospitals, universities etc.). Additionally, there are cross-functional administrations such as the county governor which for example are coordinating emergency crisis incidents that are cross-sectorial.

## 1.2 Research strategy

This research was multidisciplinary in nature, and the research targeted to undertake a series of case studies combined with systematic review of the current theoretical perspectives and best practices regarding information-and cyber crisis management, information- and cyber security training and information-and cyber security education in situational awareness and crises readiness. Moreover, the research focused on three important aspects: 1) Social versus technical aspects, 2) competence and maturity in management at different levels and units of organizations in regard to escalation and roles in handling cyber-attacks, and 3) training for resilience.

The Cisco-study from 2018 (Cisco, 2018) found that in many information-and cyber security problems, only 26% of the issues can be addressed by technology solutions alone. Ackerman argued already back in 2000 that “there is an inherent gap between the

social requirements of computer supported cooperative work and its technical mechanisms" (Ackerman, 2000), so this is not a new problem.

> "The social–technical gap is the divide between what we know we must support socially and what we can support technically." (Ackerman, 2000)

In this research project this gap has been addressed with what can be referred to as socio-technical approaches. These approaches have been used and developed with a variety of socio-technical models to analyze the gaps and find the root causes of the information-and cyber security problems mentioned above.

The "objective of socio-technical design has always been the joint optimization of the social and technical system" (Mumford, 2006), and the early motivation for developing socio-technical theories was initiated by the desire to improve industrial-workers' stationary and repetitive job situations (Mumford, 2006). In this research the motivation has been to close the socio-technical gap of resilience in the society and readiness in crisis management handling and create a framework to support those in the situation of making crisis decisions.

> "The historic structure, within the civilian, military, and government organizations, treats cybersecurity as an IT problem - not an operational one." (Østby, Lovell, et al., 2019)

The incident response perspective is still fixed in this approach, and not in the actual scope of organizational incident responsibility (Dumitru, 2016). Various challenges of learning crisis management are outlined by Lagadec (1997), and present some "barriers that emerge during the process of developing satisfactory learning practices" (Lagadec, 1997). Challenges as 1) how to detect and understand emerging crises in complex organizations, 2) to manage multi-component systems, 3) deal with expert uncertainty, 4) to handle and act in media-interest, and 5) rethink fundamental questions in increasingly unknown territory. And that

> "untrained crisis teams have little chance of finding their way through the brave new world of contemporary crises." (Lagadec, 1997)

Consequently, there is an ongoing need for training, not only to uncover flaws in regulations and emergency plans, but also by "shocking the organizations" by situations where they are not that robust (Lagadec, 1997).

In this research project these issues have been addressed with a User-centered design (UCD) process (Usability.gov, 2021), where a preparation for exercises process based on needs in the targeted organizations to deal with socio-technical vulnerabilities, and differential organizational crisis managment maturity levels is suggested (Østby & Kowalski, 2020). In addition, the issues have been approached with full-scaled exercises under supervision and trained by EXCON-teams trained in both societal and cyber-crisis incident responses (Østby, Lovell, et al., 2019).

To create learning artifacts for the 'right' level of maturity any organization are at, escalation maturity surveys (Wahlgren & Kowalski, 2016) were chosen as the measuring

instrument. Maturity modeling as a concept was first applied in the late 1970s, with the Crosby's maturity grid for quality management (Saavedra et al., 2017), and later in models like the Capability Maturity Model (CMMISM, 2002) where the goal was to encourage process improvement in organizations based on the organization's maturity. Such an escalation maturity survey was used in a case study at the Inland Hospital trust (Østby & Katt, 2019b). In the Hospital trust escalation maturity survey (EMM-study (Wahlgren & Kowalski, 2016)) (Østby & Katt, 2019b), the level of the attributes in the organization were tested to design the preparedness work before exercises (Østby & Kowalski, 2020) and before improvement work could be initiated in the organization (to start at the right level) (Østby et al., 2020). In addition, not only were the maturity measured before the exercises, but also vulnerabilities, threat assessments, plans for emergencies and contingencies were assessed to prepare for the lectures and exercises (Østby & Kowalski, 2020). The Wahlgren & Kowalski EMM (2016) was also used to study the level of maturity as part of the evaluation of the incident and crisis management in Østre Toten municipality in the aftermath of the massive cyber-attack they experienced.

To meet the resilience- and readiness gap (figure 1) a variety of learning artifacts were introduced in the exercises. The learning artifacts introduced has been e.g., socio-technical scenarios (Østby, Berg, et al., 2019), crisis management responsibilities (Østby & Katt, 2019a), or sustainability goals (Østby & Kowalski, 2022a). Different learning approaches from literature were suggested to implement the learning artifacts (Østby et al., 2020).

## 1.3 Objectives: Research goals and questions

Digitalization appears to require a more complex risk- and resilience analysis process than those that society have been using in the past (Haimes, 2009). Communication to the public sector to enhance the understanding and the significance of information- and cyber-security and safety within public services is therefore required to improve the resilience and readiness of the consequence's socio-technical cyber-attacks may have.

Additionally, people have become more liberal on what information they share about themselves, and what information others collect about them (Norwegian Data inspectorate, 2018). Many citizens have indicated a certain discomfort by the fact that their personal information is on foreign hands, but they may still not be aware of what the consequences can be. There are in addition newspaper-articles that describe outsourcing of the municipalities health care systems to larger production units outside the municipality area of control (Jørgenrud, 2017). One of the major goals of this research has therefore been to **explore consequences of inadequate cybersecurity measures used by municipalities and other public emergency organizations that lead to cybersecurity failure and inadequate response by those who are responsible in these organizations**.

To better understand the scope and magnitude of the problem three research questions were proposed to establish the status and outline a foundation to model and measure and manage cybersecurity posture in relations to public safety and security:

Research question (RQ) 1
Is the connection between digitalization and civil protection sufficiently consolidated in emergency readiness and preparedness plans of public emergency organizations to deal with cyber systems failures regarding either accidental or malicious incidents?

> *RQ 1: What is the current level of resilience and readiness in public emergency organizations regarding cyber systems failures?*

Research question (RQ) 2
Current research indicates that governmental maturity in different departments and organizations within a country differs (G. Karokola et al., 2011; Wahlgren & Kowalski, 2016), and that before generalized country wide cybersecurity solutions can be adopted there is a need to first understand the gaps between different departments and organizations, and to understand the current escalation maturity levels of relevant departments and organizations in the Norwegian public services.

> *RQ 2: What is the current level of readiness within different and relevant departments and organizations in relevant public emergency organizations?*

Research question (RQ) 3 A
Once the current status had been established on both information- and cybersecurity preparedness and resilience in relevant public emergency organizations, e.g., EMMs, we searched and developed suitable methods and tools to establish and maintain the information- and cybersecurity knowledge needed by organizations to purchase, build, and operate, resilient, digital value chains. The Norwegian law concerning the municipality's emergency duty, civilian preparedness and the Civil defense organization (Justis- og beredskapsdepartementet, 2010), presents the municipalities' concrete responsibility in this matter. The third research question was therefore based upon the municipality responsibility:

> *RQ 3 A: What are the suitable methods and tools to establish, maintain and communicate information- and cybersecurity knowledge to Norwegian counties and municipalities within information- and cybersecurity risk and resilience work?*

Even though crisis domain is similar to, for example healthcare, adverse events occur much less often. While crisis research relies substantially on simulation, healthcare learns from first-hand experience daily. This makes healthcare a source of insight about worker and work team responses to challenges. It also provides a more effective way to validate decision support procedures and new ICT prototypes (Nemeth et al., 2011). A secondary goal of this research was therefore to **establish overviews of risk-and resilience work and emergency preparedness caused by cyber systems failures in relevant levels of government emergency organizations.**

To better understand the scope and magnitude of this second research goal, two research questions were established to meet the goal:

Research question (RQ) 3 B
We needed to search for best information and training-practice in other countries which have developed information- and cybersecurity emergency preparedness and resilience in digital value-chains. There was also a need to study what digital risk- and resilience that already exist (if any) in the Norwegian organizations, to see if there are any suitable methods which can be transferred to overall information- and cybersecurity risk- and resilience. Research question 3B was therefore formulated as:

> *RQ 3 B: What information systems and training within digital risk- and resilience value-chains can be suitable to reach out to different management levels in the hierarchies in the government emergency organizations?*

Research question (RQ) 3 C
The current EMMs among leaders in government emergency organizations was established from RQ 2. RQ2 depended also on the knowledge from RQ 3 B, and we therefore waited with RQ 3C till we got the results from the combination of RQ2 and RQ 3 B. This resulted in suggested changes in how we should model our emergency-departments both in human resources and in information- and cybersecurity-incident-handling, and research question 3 C was therefore formulated as:

> *RQ 3 C: What methods can be developed and possibly modeled to ensure better information- and cybersecurity-incident-readiness and information- and cybersecurity emergency preparedness to leaders in public emergency organizations?*

## 1.4 Thesis summary overview

After this introduction, the chosen methodology for the research, together with some ethical, academically, and societal considerations are presented. Thereafter, the summary of results is discussed, before a rigor and relevance chapter is outlined. Finally, some concluding remarks and ongoing and future research directions are presented. The thesis summary is presented orderly based on the pragmatic research methodology design science research in information security (DSRIS – see section 2.1), as presented in figure 2.

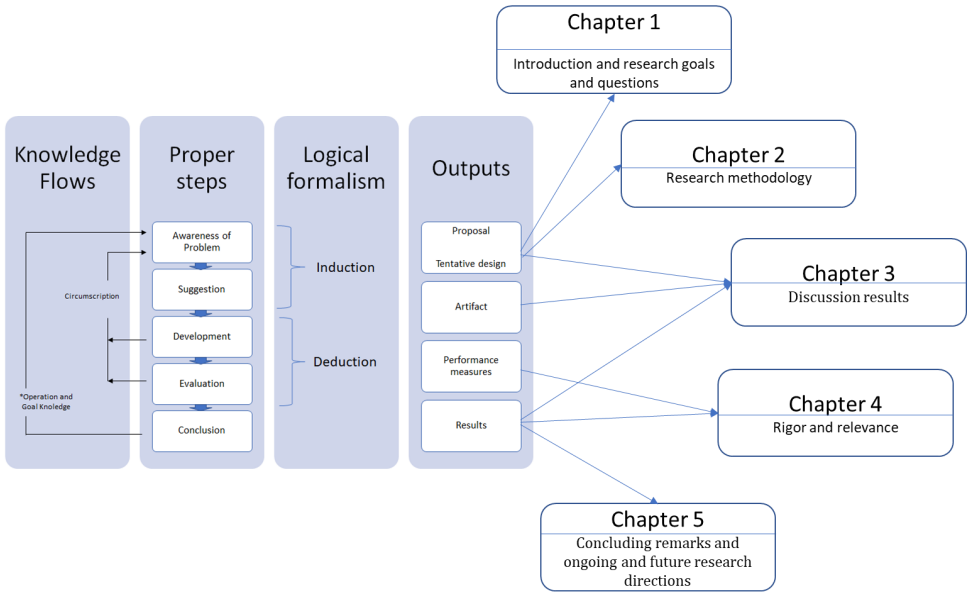



**Fig. 2.** Chapter overview

# 2 Research Methodology

Given the broad scope of this research work, it has been important to apply suitable approaches to develop methods that could close the socio-technical resilience and readiness gap efficiently and effectively. A generic research onion process (GROP), shown in figure 3 below, has been used to systematically choose the appropriate methodologies.

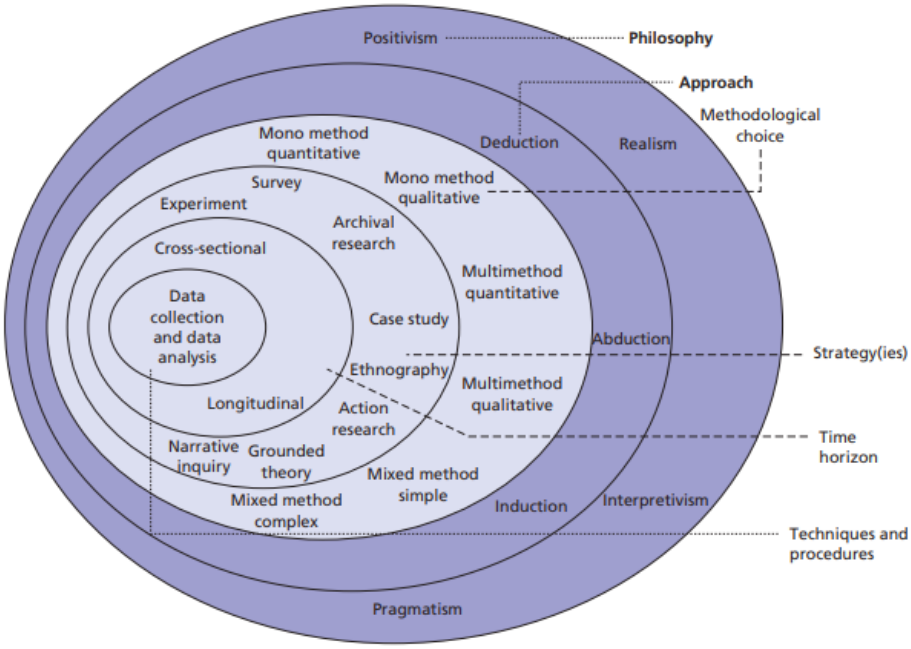



**Fig. 3.** The research 'onion' (Saunders et al., 2012)

This chapter is structured as follows; 2.1) research philosophy, 2.2) research approach, 2.3) methodological choice and scope, 2.4) time horizon, 2.5) research strategies and research data sampling, 2.6) data analysis, 2.7) ethical academically and societal considerations, and finally 2.8) a brief summary with an overview of the chosen methodology.

Each section describes how the different 'onion' layers are applied in the research work, and how research sample selections have been combined.

## 2.1 Research philosophy

To meet the goal to model and/or develop learning artifacts for todays and future leaders to improve the information- and cybersecurity crisis response and management preparedness, the pragmatism philosophical perspective was chosen for this research project.

A pragmatism philosophical perspective can be referred to as methodology where multiple views to reality that best fit the research questions are used (ontology).

Moreover, where observable phenomena or/and subjective meanings provide acceptable knowledge to the research questions (epistemology). And finally, where values (subjective or objective stance to understand and describe the situation) play an important role in interpreting results (axiology) (Saunders et al., 2012). In a pragmatism philosophical perspective, the data collection methods can be mixed or multiple, quantitative, and qualitative, to best meet the research questions (Saunders et al., 2012). An overview of research philosophies marked with the selected pragmatism view are presented in table 3.

**Table 1. Comparison of research philosophies (Saunders et al., 2012)**

| | **Pragmatism** | **Positivism** | **Realism** | **Interpretivism** |
|---|---|---|---|---|
| Ontology: the researcher's view of the nature of reality or being | External, multiple, view chosen to best enable answering of research question | External, objective, and independent of social actors | Is objective. Exists independently of human thoughts and beliefs or knowledge of their existence (realist), but is interpreted through social conditioning (critical realist) | Socially constructed, subjective, may change, multiple |
| Epistemology: the researcher's view regarding what constitutes acceptable knowledge | Either or both observable phenomena and subjective meanings can provide acceptable knowledge dependent upon the research question. Focus on practical applied research, integrating different perspectives to help interpret the data | Only observable phenomena can provide credible data, facts. Focus on causality and law-like generalizations, reducing phenomena to simplest elements | Observable phenomena provide credible data, facts. Insufficient data means inaccuracies in sensations (direct realism). Alternatively, phenomena create sensations which are open to misinterpretation (critical realism). Focus on explaining within a context or contexts | Subjective meanings and social phenomena. Focus upon the details of situation, a reality behind these details, subjective meanings motivating actions |
| Axiology: the researcher's view of the role of values in research | Values play a large role in interpreting results, the researcher adopting both objective and subjective points of view | Research is undertaken in a value-free way, the researcher is independent of the data and maintains an objective stance | Research is value laden; the researcher is biased by world views, cultural experiences and upbringing. These will impact on the research | Research is value bound, the researcher is part of what is being researched, cannot be separated and so will be subjective |
| Data collection techniques most often used | Mixed or multiple method designs, quantitative and qualitative | Highly structured, large samples, measurement, quantitative, but can use qualitative | Methods chosen must fit the subject matter, quantitative or qualitative | Small samples, indepth investigations, qualitative |

*Design science research for information systems (DSRIS)* methodology was adopted as a pragmatism research philosophy approach in this research project.

> "Design science research in information systems (DSRIS) is a methodology which can be conducted when creating innovations and ideas that define technical capabilities and product through which the development process of artifacts can be effectively and efficiently accomplished" (Kuechler & Vaishnavi, 2012)

DSRIS as presented in figure 4 have been used to develop learning artifacts.

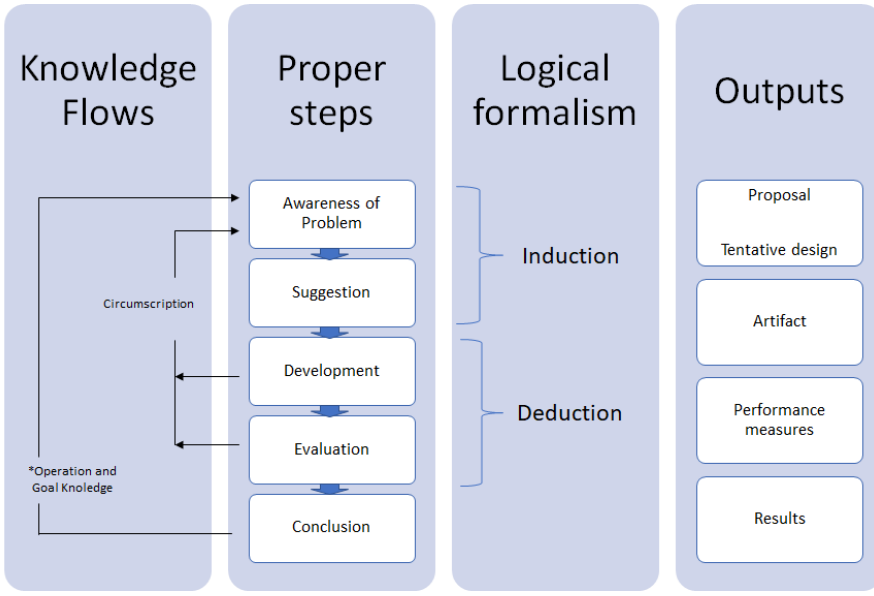



**Fig. 4.** Design research methodology in information systems (modified) (G. R. Karokola, 2012)

Instead of only defining the technical capabilities, multiple views as in socio-technical approaches have been adapted to the DSRIS. For this research, no new socio-technical models have been suggested. Instead, traditional dynamic socio-technical approaches, e.g., as proposed by Leavitt in 1965 and modified by Kowalski in 1994 (Kowalski, 1994; Leavitt, 1965) presented in figure 5 has been adapted to both the induction and deduction phase of the logical formalism section of the DSRIS.

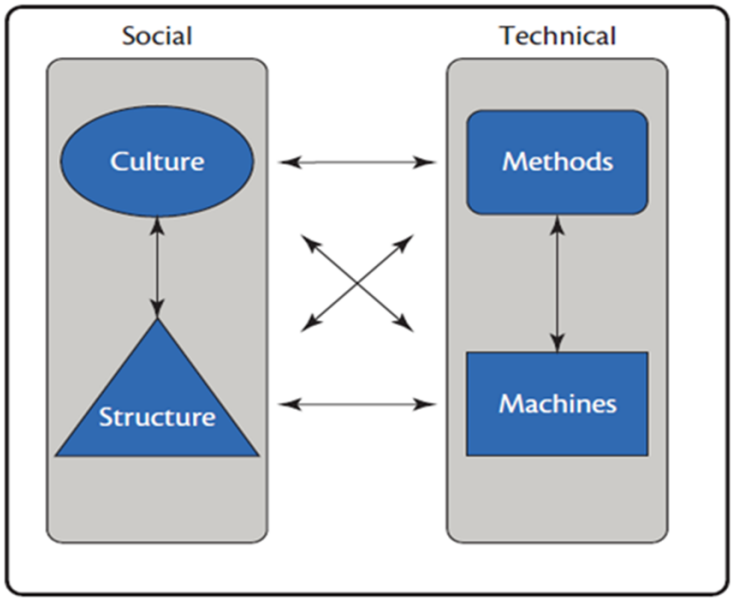



**Fig. 5.** Socio-technical approach (Kowalski, 1994; Leavitt, 1965)

The logical formalism process of the research project has also been adapted to meet the epistemology of the pragmatic philosophical dependencies of the research questions, starting out with an inductive approach to observe cases. Thereafter the suggestions and development have been evaluated through deductive processes. An overview of these logical formalism approaches is presented in table 2.

**Table 2. Abduction, deduction, and induction approaches (Koingharara, 2022)**

| | **Abduction** | **Deduction** | **Induction** |
|---|---|---|---|
| Premiss | Fact | Rule | Case |
| Premiss | Rule | Case | Fact |
| Outcome | Case | Fact | Rule |

These modifications (multiple views in both social and technical approaches, and induction approach as a starting point) to the DSRIS and how they apply to the pragmatic philosophical approach are presented in table 3.

**Table 3. DSRIS as a pragmatic philosophical approach**

| | Pragmatism | Modified DSRIS |
|---|---|---|
| Ontology: the researcher's view of the nature of reality or being | External, multiple, view chosen to best enable answering of research question | Multiple (socio-technical) realities enabled |
| Epistemology: the researcher's view regarding what constitutes acceptable knowledge | Either or both observable phenomena and subjective meanings can provide acceptable knowledge dependent upon the research question. Focus on practical applied research, integrating different perspectives to help interpret the data | Knowledge is created through design, combining subjective ideas with relevant acceptable knowledge dependent on the research question |
| Axiology: the researcher's view of the role of values in research | Values play a large role in interpreting results, the researcher adopting both objective and subjective points of view | Values play role in designing (learning artifacts), improvement and understanding |
| Data collection techniques most often used | Mixed or multiple method designs, quantitative and qualitative | Participation in designing suggestions, quantitative and qualitative evaluation from exercises, case studies, and literature review |

## 2.2 Research approach

To collect data to develop (theoretical) framework can be referred to as grounded theory. More specifically "the discovery of theory from data" (Glaser & Strauss, 2017). Given the emergent need for information security training (Cisco, 2018) that was targeted in this research project, it has been important to identify and apply suitable research approaches that are innovative, applicable for learning, and to create a malleable environment.

This research was approached using aspects of grounded theory that can be referred to as a naive inductivist approach. The naive inductivist approach starts by first observing a phenomenon and then generalizing about the phenomenon which leads to theories that can be falsified or validated (Chalmers, 1999; Kowalski, 1994). The approach is presented in figure 6.

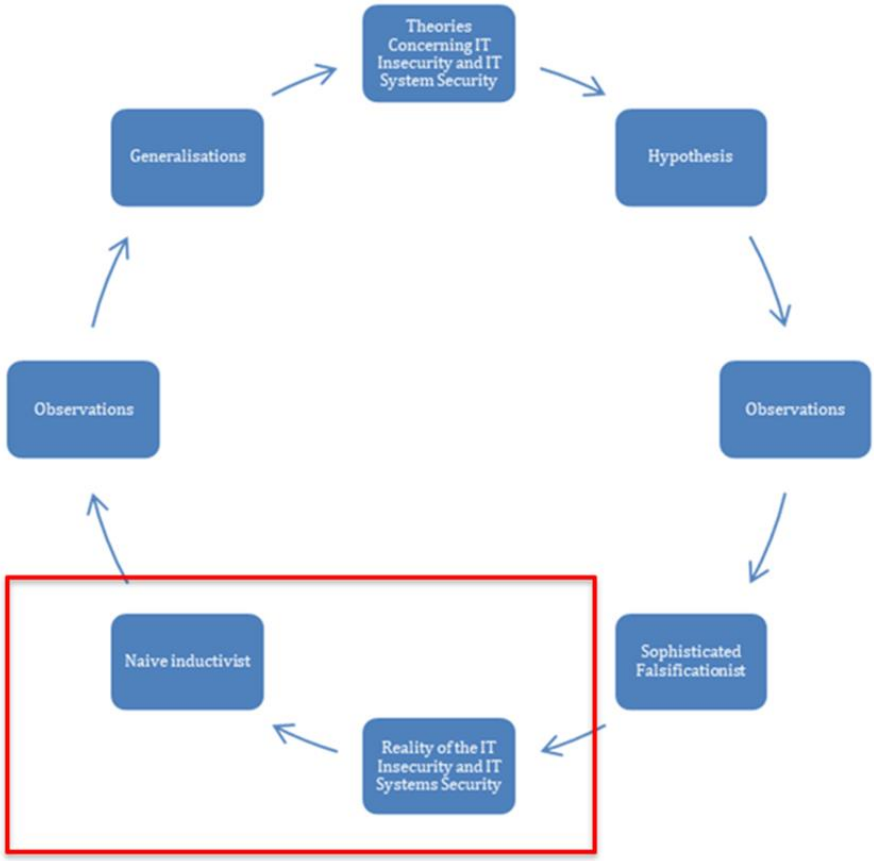



**Fig. 6.** Naive inductivist approach (Chalmers, 1999; Kowalski, 1994)

## 2.3 Methodological choice and scope

Multiple mixed methods (Saunders et al., 2012) have been used to meet the goals of this research. To meet the goal regarding **resilience and readiness in municipalities and other public emergency organizations,** the scope was framed to target hospital trusts and municipalities in Norway, and case-studies and qualitative and quantitative surveys and interviews were executed in these organizations. To meet the goal to develop **suitable methods to close the gap** the scope was framed to investigate information- and cybersecurity-management in the **public emergency organizations** in both the organizations themselves and information- and cybersecurity-operations centers, and quantitative and qualitative collection of data from surveys and other preparation information needed (Østby & Kowalski, 2020) were used to prepare for and execute information- and cybersecurity crises exercises. Moreover, quantitative, and qualitative methods as hotwash-sessions and survey-evaluations were used to evaluate the exercises.

On a day-to-day basis, information- and cyber-security in the Norwegian civil public sector is regulated under the jurisdiction of the Justice department. Consequently, public protection and public emergency organizations within this jurisdiction were chosen as the scope of the research. A limitation of this choice, especially when writing scenarios for exercises (in the nature of cyber-attacks crossing borders), especially when presenting and discussing malicious cyber-attacks, is that the Military defense and the Military forces were not included in the context of the research focus. The focus was however on what impact these types of attacks have on the civil society overall.

Several parties were involved in the research, such as The Innlandet Hospital trust (Sykehuset Innlandet), Ahus (Akershus Universitetssykehus), Sykehuspartner, DSB (The Norwegian directorate for civil protection), NSM (The Norwegian National Security Authority), The Norwegian Digitalization directorate, NorSIS, Gjøvik municipality, Østre Toten municipality, NTNU (The Norwegian University of Science and Technology), Stonepaperscissors, The Innlandet county governor, The Innlandet exercise council (led by the Innlandet police district), The Innlandet police district, Kripos, and the JusticeCERT. What projects these were involved in or participated in, and potential effects of those, are presented in table 4.

**Table 4. Project, participants, and potential effects**

| Project | Participants | Potential effects |
|---|---|---|
| Case study 1: MM at the Innlandet Hospital trust | 8 | Measuring level of information security to prepare for 1) exercises and 2) step-by-step approaches |
| Case study 2: Gjøvik municipality prevention case | 4 | Root-cause analysis using socio-technical incident response systems |
| Case study 3: Cyber-attack handling in Østre Toten municipality | 28 in survey, 9 in depth interviews | Publicly available report. Measuring cyber-attack handling based on text-book theories, socio-technical incident response systems, and laws and regulations. Open ended questions in depth-interviews. |
| Crisis management exercise with IT-management group at NTNU | EXCON-team of 5, and 11 participants | Crisis management resilience and readiness. |
| Student-exercises IMT-4115 | EXCON-team of 3, participants:<br>Year 1, day 1: 70<br>Year 1, day 2: 13<br>Year 2, day 1: 120<br>Year 2, day 2: 10 | Triple-loop-learning in exercises. Learning artifacts for students to bring forward. |
| ovelse.no with DSB (The Norwegian directorate for civil protection), NSM (The Norwegian National Security Authority), The Norwegian Digitalization directorate, and NorSIS | Project group (from the organizations mentioned) and development-team run from NCR/NTNU | Information security discussion exercises for all organizations in Norway |
| Atlantic council 9/12 cyber-security challenge | Participation in team, coaching a team, being judge | Serious games as a master course |
| Megagame at the security-festival in Lillehammer with Stonepaperscissors | Game-master team of 10, and 77 participants | Societal impact from crises. Sustainability. |
| Test-exercise at the Norwegian Cyber Range, with EXCON team from NTNU/NCR, Innlandet County general, The Norwegian Army, and the Innlandet hospital trust | EXCON-team of 11 and 14 participants (students) | Train the trainer experience. Crisis management resilience and readiness. |
| Policy-exercise with CCIS-partners, with EXCON and administration help from FFI, The Norwegian Army's Cyber Defense, NTNU/NCR, NTNU Media and the Innlandet county governor | EXCON-team of 12 and 58 participants | Information to CCIS-partners about the NCR. Crisis management resilience and readiness. |
| Full-scaled exercise with Ahus and Sykehuspartner, EXCON team from NTNU/NCR, Ahus, Sykehuspartner, NTNU Media | EXCON-team of 14 and 38 participants | Crisis management resilience and readiness. |
| Information sharing exercise with SIKT (exercise Morris) | EXCON-team of 16 +14 local exercise leaders, and 144 participants | Survey amongst local exercise-leaders, and one for all participants. Skills from sharing sensitive information in crisis. Information about tools and platforms. |
| Crisis management exercise with management group in Kripos, EXCON-support from Innlandet police district, justiceCERT, IT-group in Kripos, and NorSIS | EXCON-team of 9 and<br>14 participants | Crisis management resilience and readiness. |

The studies have, to some extent, been limited to the scope of enquiry to public organizations such as municipalities and diverse sectorial emergency organizations in Norway.

## 2.4 Time horizon

As this research project is multidisciplinary in nature, a cross-sectional approach was selected to meet the research questions. The student exercises in the IMT-4115 course can however be considered as a longitudinal cohort study, as it has been executed in the same format over a three-year period (Østby & Kowalski, 2022b).

## 2.5 Research strategies and research data sampling

The research strategy in this project, being inductive and grounded in its approach, started out as explanatory and descriptive research, but has also undertaken exploratory research to validate the explanatory and descriptive research.

> "Studies that establish causal relationships between variables may be termed explanatory research." (Saunders et al., 2012)

Case-studies performed using socio-technical 'relationships' models to analyze the relations between different variables has been used in this research.

> "The case study strategy has considerable ability to generate answers to the question 'why?' as well as 'what?' and 'how?' questions. For this reason, the case study strategy is most often used in explanatory and exploratory research." (Saunders et al., 2012)

Several of the questionnaires in this research have however asked about the respondent's views on the organizations work on specific tasks.

> "Descriptive research tends to undertake attitude and opinion questionnaires and questionnaires of organizational practices" (Saunders et al., 2012).

This being combined with what category (categorical data) the respondents are a part of, have in this project given results which are different in the example strategic, tactical, and operational layers, and foundation for what to train (and explore) in e.g., exercises.

Categorical data can be described as

> "data whose values cannot be measured numerically but can be either classified into sets (categories) according to the characteristics that identify or describe the variable or placed in rank order" (Berman Brown & Saunders, 2008)

In this project this would e.g., be the mentioned categories strategic, tactical, and operational layers in an organization.

In an exploratory study, qualitative precedes quantitative (Saunders et al., 2012), and in this research process has been used to validate the explanatory and descriptive data.

We had a master-student to do in-depth-interviews (qualitative) with experienced Norwegian exercise control (EXCON)-leaders on how they train new EXCON-members

(Selebø, 2022). In addition, participatory action research was executed to validate suggested frameworks for preparation and execution of exercises.

The data sampling in this thesis summary is presented in table 5, with 1) the research questions, 2) the publications relevant for the research question, 3) if there are some relevance from the Østre Toten report (appendix 1) to the research question, 4) if there are some comments to the publications in the thesis summary relevant for the research question, 5) if it is explanatory, descriptive, or exploratory method used for the research questions, 6) which DSRIS-steps are executed in the different research questions, and 6) what study-subject targeted or study-environment these were executed in.

Each research question is mapped to the most relevant research question. This is presented in the order the publications are presented in this thesis summary. If the results from Østre Toten public report is relevant for the research question and discussed in this thesis summary, it is marked with a V, as is also if there are comments in the results and rigor and relevance chapters to the publications in the thesis summary. Whether it has been used explanatory, descriptive, or exploratory research within the research questions, it is also marked with a V. Which steps in the DSRIS that are executed within the different research questions are presented in a separate column, and so is also what type of study subject/environment.

**Table 5. Research questions, publications, and activities**

| Research | | | | Applied research methods and strategies | | | DSRIS steps | Study subject/ environment |
|---|---|---|---|---|---|---|---|---|
| RQ | Publications | Public report | Thesis summary comments | Explanatory | Descriptive | Exploratory | | |
| 1 | 1 & 2 | V | V | V | V | | Awareness and suggestions | Municipalities, Hospital trust, and literature search in PhD course |
| 2 | 2 & 6 | | | V | | | Awareness, suggestions, and development for tentative designs | Hospital trust |
| 3A | 2, 3 and 4 | V | V | V | V | | Evaluation, circumscription for new suggestions, evaluations, proposals for artifacts | Hospital trust, Student-exercises, and Municipality responsibility study |
| 3B | 3, 5, and 6 | | V | | V | V | Performance measures and suggestions for development, and artifacts and results | Student-exercises, Discussion exercises, Games, Table-top, Full-scaled exercises, and preparation for the exercises |
| 3C | 6, 7, and 8 | | V | | V | V | Suggestions, development, evaluation, and conclusions for results | Preparation for exercises, developing EXCON-teams, developing learning goals through scenarios in the exercises |

The focus and most of the work has been executed towards the development and evaluation of the suggested artifacts. Working on the development and experiencing the results do often trigger new possibilities, but the experiences have also confirmed the relevance and the potential of the results found and published from the research.

Regarding the RQ1 and RQ2, data was collected from Gjøvik municipality, The Innlandet hospital trust, Østre Toten municipality, and Ahus hospital trust, which was analyzed and processed to understand current status and suggest artifacts. In addition, a literature review was performed to find the current status of research within the scope of the research. Regarding the RQ 3A, 3B, and 3C data were collected from 1) Innlandet hospital trust, 2) Østre Toten municipality, 3) results from evaluation of ovelse.no, 4) results from

evaluation of student exercises, and 5) results from participatory action research from table-top and full-scaled exercises at the Norwegian Cyber Range.

## 2.6 Data analysis

To analyze the data from the case-studies, 1) socio-technical root cause analysis, 2) categorical analysis from descriptive data/results questionnaires and expected/not expected or yes/no questions (dichotomous descriptive data), and 3) qualitative effect analysis from the variety of actions used for triple-loop-learning processes, where used to re-plan exercises. These are explained in the following three sections.

### 2.6.1 Socio-technical root-cause-analysis

A root-cause analysis tool is designed to help identify

> "not only what and how an event occurred, but also why it happened .. to determine why an event or failure occurred .. and to be able to specify workable corrective measures that prevent future similar events." (Rooney & vanden Heuvel, 2004)

Such analysis is used to investigate and categorize the root causes of events with a variety of impacts. In this regard, the term "event" is used to describe occurrences that "produce or have the potential to produce" consequences to safety, health, environmental, quality, reliability, and production (Rooney & vanden Heuvel, 2004). If the event is caused by e.g., system attacks (technology), both the system-attacks themselves and the consequences need to be analyzed.

> "For the analysis of functioning artifacts in context, the combination of 'the social' and 'the technical' is the appropriate unit of analysis." (Geels, 2005)

A socio-technical root cause analysis can therefore be described as a tool to identify both 'the social' and 'the technical' aspects of an event.

Socio-technical root-cause-analysis were used and discussed in the following research publications and case-studies 1) in the Gjøvik municipality case (Østby & Kowalski, 2021) (publication 1), 2) in the discussion for serious games as a master course (Østby & Kowalski, 2022a) (publication 5), 3) in the discussion for preparation process for exercises framework (Østby & Kowalski, 2020) (publication 6), 4) and finally in the scenario-for-exercises framework (Østby, Berg, et al., 2019) (publication 8).

In publication 1 and 8 such root-cause analyses were used, while publication 5 and 6 have discussed how to use such, as a part of the framework presented. A socio-technical root-cause analysis (based on publication 1) was also used in the Østre Toten municipality case study (Østby & Kowalski, 2022c).

### 2.6.2 Descriptive categorical data analysis

To create a foundation for changes, descriptive data had to be either adapted or developed to be analyzed.

To analyze the maturity levels in the organizations, already existing descriptive data were used. EMM-questionnaires were executed to find the differences between strategic, tactical, and operational levels in the organization. In the EMM-questionnaires, there were only two categories: Yes and No, for each question. "These are known as dichotomous data, as the variable is divided into (only) two categories." (Saunders et al., 2012) In this case we were able to analyze the differences on the different layers in the organization (Østby & Katt, 2019b).

Evaluation-questionnaires were constructed to observe if the learning goals in the scenarios were met. The questions included learning goals that were not directly actioned in the scenario- for example logistics, and we could analyze if the actual learning goals were met. To analyze the preparation process for exercises, the evaluation/after-action-review were constructed to analyze the exercise-goals from the exercise-directive by the participants.

To analyze the execution of the exercises, the EXCON-teams also evaluated how they met the exercise-goals, so the EXCON-team can in this regard also be seen as a category in itself (Østby et al., 2022; Selebø, 2022). They did however only participate in the after-action-review, and the categorization of the data is therefore not as easily analyzed as for the participants who also did the surveys. In the student-exercise however, all the deliveries/assignments in the exercise were reviewed and I could thereby find "flaws" in my own communication and templates (i.e., when for the nb. 2 exercises the first year, half of the groups used a wrong template, and second that some groups in both exercises the first year misinterpreted one of the templates), which lead to changes in both communication and templates.

### 2.6.3 Thematic exploratory analysis and participatory action research (qualitative analysis)

Usually in exploratory studies, qualitative precedes quantitative (Saunders et al., 2012), but in this research exploratory studies have been used to validate the explanatory and descriptive data.

Thematic analysis can be exploratory in their nature, and for the in-depth-interviews in Selebø's master thesis (Selebø, 2022) a thematic text-analysis from the transcripted interviews were executed. The analysis of the literature review was also executed in a thematic way.

Participatory action research is also a class of exploratory analysis, that is being qualitative in its nature.

> "Participants have special access to how social and educational life and work are conducted in local sites by virtue of being 'insiders', … and that insiders have special advantages when it comes to doing research in their own sites

and to investigate practices that hold their work and lives together in those sites—the practices that are enmeshed with those sites." (Kemmis et al., 2014)

When participating in the exercises as an instructor (or as the teacher/administrator in the student-exercise), the participatory action research method to 1) plan, 2) act, 3) observe, 4) reflect and 5) re-plan in a spiral ongoing in the exercise where used. The participatory action research method is presented schematically in figure 7.

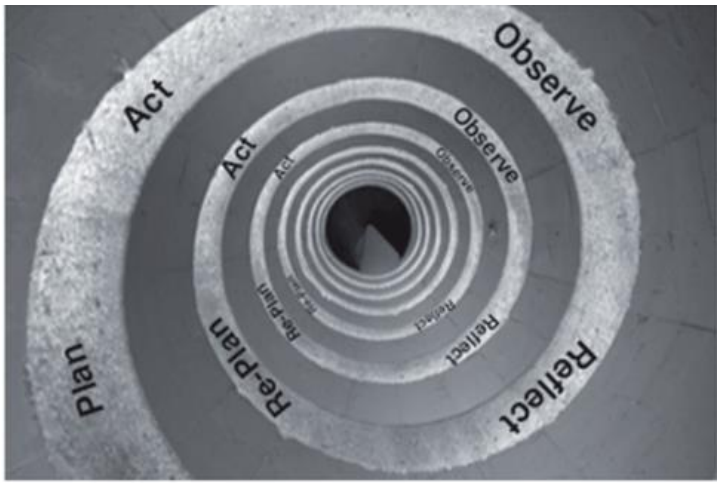



**Fig. 7.** The action research spiral (Kemmis et al., 2014)

An example of reflection and replan of how to execute full-scaled exercises are presented in chapter 3, figure 23 in this thesis summary. Changes in the student-exercise from year 1 to year 2 are presented in the publication (Østby & Kowalski, 2022b) (publication 3). Regarding the student-exercise, we also (in addition to what is explained in the publication) made technical changes in the learning-platform, such as automatic registration when entering the scheduled session and wider timeline for assignments (deadline 15 minutes later than scheduled). These technical changes made the acting part of executing the exercise easier, as we now don't need to 'count' the participants, and there are no personal-email deliveries as it was the first year. In a triple-loop-learning context, these types of participatory reflection led to transformative changes.

## 2.7 Ethical academically and societal considerations

The quantity of personal information and system vulnerabilities we obtain when executing exercises for organizations at NCR have required necessary preparation to secure the information. Both NDA's (Non-Disclosure Agreements) and data-redaction (immuta.com, 2021) to protect the organizations' vulnerabilities are at all times considered. The rules of Norwegian Centre for Research data (NSD), and NTNU's regulations for research have always also been considered and used when required.

There were a number of ethical issues that were faced during this research project. One example is the maturity-study at the Inland hospital trust, where there was date and time for the executed replies in the pc, which could be traced back to booked times for the participants (also top management as mentioned). In this case we planned for the

timeline of the study and used the regulations from NSD. Information letters with consent were used, and we were able to execute the study according to ethical standards needed. Another example was how to practically secure ovelse.no users (0 trace possibilities backwards from the online questionnaire) and their participation in the evaluation-survey. In this case we decided to use Norwegian personal identification log-on to the system in addition to registration of organization number to identify the type of organization in the evaluation study.

## 2.8 Summary

The Design Science Research in Information Security as a pragmatism philosophical perspective was chosen for this project to develop learning artifacts to close the resilience and readiness gap in public emergency organizations. The research was approached with a naive inductive approach, and the strategy has been to meet the challenges with multiple mixed methods, and several public emergency organizations have been invited to take part in the research. Mostly, the studies have been cross-sectional, but the student-exercise have been executed over a 3-year period (longitude). The collection of data was initially done explanatory and descriptive, but exploratory data collection was collected to discuss and validate the findings. To analyze the data, socio-technical root-cause-analysis, categorical analysis from descriptive data/results questionnaires and expected/not expected or yes/no questions (dichotomous descriptive data), and qualitative effect analysis from the variety of actions, were used. An overview of the research methodology is presented in table 6.

**Table 6. Research methodology**

| **Research methodology** | **Choice** |
|---|---|
| Research philosophy | Pragmatism: DSRIS |
| Research approach | Naive inductive approach |
| Research strategy and scope | Multiple mixed methods |
| Time horizon | Cross-sectional approach (one longitude) |
| Data collection methods | Explanatory, descriptive, and exploratory collection of data |
| Data analysis methods. | Root-cause-analyses using socio-technical models, categorical analysis from descriptive data/results questionnaires and expected/not expected or yes/no questions (dichotomous descriptive data), and qualitative effect analysis from the variety of actions used for triple-loop-learning processes |

# 3 Discussion results

The research strategy of this project was first and foremost to create a variety of learning artifacts to improve the resilience and response capabilities in public emergency organizations. The results from the project are therefore both of relevance for the society and public emergency organizations, but also for more rigorous academic research.

The dissemination plan for this doctoral research project were therefore the following 1) publications and publicity, 2) information security awareness in society, 3) develop best practice procedures, courses and exercises, 5) establish collaboration between NTNU and governmental and operative civil preparedness and emergency departments 6) established knowledge about public emergency responsibilities and finally 7) collaboration with organizations at NTNU – especially in the cyber-range context, but also within the information security education.

In terms of publications, to date the research project has produced 9 academic publications and one extended abstract, whereas the academic publications are 6 conference publications and 3 journal publications. In addition, one public report has been produced to meet the expectations of awareness in the society and to develop procedures, courses, and exercises with the collected data (Østby & Kowalski, 2022c) (appendix 1). The project has established contact with municipalities, hospital trusts, counties, and national authorities. Establishing collaboration with these parties in EXCON-teams when arranging exercises at the NCR (Østby, Lovell, et al., 2019), NTNU and NCR also have become familiar with public emergency responsibilities.

Beyond the scientific publications, the research results were also mentioned in both a local newspaper (Horni, 2020) and in national relevant magazines like the NSO-magazine "Sikkerhet" (Kvie Lundevall, 2020) and "Aktuell sikkerhet" (Mathisen, 2021). The most interesting ones were however, when the Østre Toten municipality report (Østby & Kowalski, 2022c), and moreover, an article about the first full-scaled exercise at the Norwegian Cyber Range (Nyheim, 2022) were posted on LinkedIN. Both got proximately 10000 exposures within one week. In comparison, when attendance in Cybercation in Tartu, Estonia (ctftech.com, 2022) were posted, there were only 1250 exposures.

In the two following sections of this chapter, the case-studies are presented and discussed, before the preparation for exercises are discussed, and finally the variety of attendance at and participation and lead of exercises are presented and discussed.

## 3.1 Case studies crisis management

**The first case-study** took place at the Innlandet hospital trust (Østby & Katt, 2019b). A maturity model developed by Whalgren & Kowalski (Wahlgren & Kowalski, 2016) was used to measure escalation maturity on different layers in the organization. What was interesting is that the maturity was quite similar at the different hierarchical layers but could vary quite a lot on some attributes from one hierarchical layer to another. One of the interesting findings in this regard was the difference on reporting between the strategic layer and the operational layer. This variety is presented in figure 8.

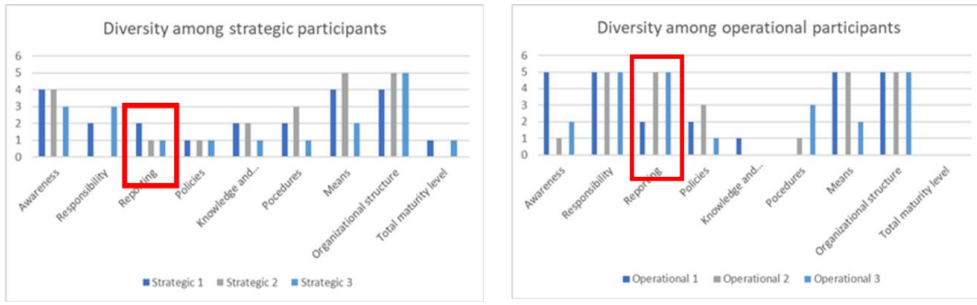



**Fig. 8.** Variety in views of maturity in reporting (Østby & Katt, 2019b)

These types of varieties were relevant to look at from two perspectives, 1) how to close the gaps, and 2) how one can approach the challenges in exercises. Suggestions for the improvement of the maturity process are present in publication 2. A method to close the gap, and how to prepare for exercises using (amongst other variables) EMM's in the preparation process (publication 6).

**The second case-study** took place in Gjøvik municipality after they suspended all email-communication in and out of the municipality based on ongoing risk of being attacked via attachments in emails (Staveli, 2020). The method used was interviews with those who took part in the decision. The case was analyzed using a combination of the identification phase in the NIST-framework (Anderson, 2017), and a socio-by-consensus (SBC)-model presented by Kowalski (1994) in combination with the socio-technical framework presented in figure 5. The SBC-model model the framework as a semiotic stack of social controls as e.g., ethics, laws, administration, and technical controls as e.g., application, operating systems, hardware (Kowalski, 1994). The NIST-framework model the risk-and incident-response in a process, covering identify, protect, detect, response, and recover (Anderson, 2017). Results from the case-study are presented in publication 1. As the case itself only covered the identification and protection phase of the NIST-framework (see figure 9), the socio-technical root-cause analysis was limited to those two phases. The results indicated however, that the root-cause analysis could be easily adapted to other information security incidents.

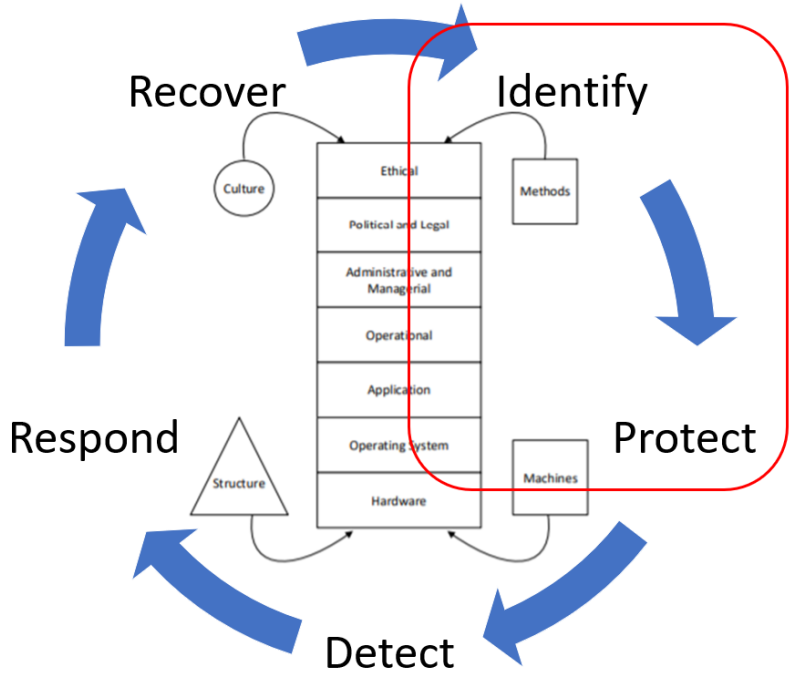



**Fig. 9.** Socio-technical root-cause analysis of the Identify and Protect phases of the NIST-framework (Østby & Kowalski, 2021).

**The third case-study** took place in Østre Toten municipality, after a ransomware-attack which encrypted 240 business systems which were in daily use in the municipality (Østby & Kowalski, 2022c). We were commissioned by Østre Toten to review the incident response in the cyber-attack. This to meet the at any time requirement from 'Instruks for statsforvalteren og Sysselmesteren på Svalbard sitt arbeid med samfunnssikkerhet, beredskap og krisehåndtering' § 5, 'Instruks for statsforvalterens oppgaver som veileder og pådriver" nb. 5 (The Norwegian Justice- and emergency department, 2015) to evaluate any types of incidents in a municipality in Norway. The results are already published in Østre Toten municipality's webpage. The mandate was to bring about awareness in the Norwegian society, and learn from the attack both within the organization, for other organizations, and to use in lectures, training, and exercises. The methods used to collect data were firstly a questionnaire using 1) Whitman & Mattord content of information security crisis management (2018), 2) socio-technical questions as in the Gjøvik municipality case (Østby & Kowalski, 2021) (publication 1) but for the respond and recovery phase, 3) questions about national regulations (DSB, 2018; Justis- og beredskapsdepartementet, 2010), and 4) the Wahlgren & Kowalski MM escalation model (Wahlgren & Kowalski, 2016). Secondly, in-depth-interviews were executed. In the in-depth-interviews questions were asked about involvement, responsibilities (roles/tasks), actions and what was learned from the incident management. In total 28 of those involved in the crisis management answered the questionnaire and 9 in depth-interviews were executed.

The main findings from the Østre Toten study are listed below. The list has been adapted and translated from the report which originally is in Norwegian – appendix 1 (Østby & Kowalski, 2022c).

1) Cyber-attacks require a separate place on the organization's risk and vulnerability list (cannot be considered as power outages or e-com failures).
2) External information requirements are extraordinary, different, and more demanding than in a "normal" incident (e.g., from national security organizations, intelligence service organizations, CSIRT, data protection authority etc.).
3) Contingency plans must include a plan for and contract with an external ICT incident management and recovery team (if such personnel are not part of the organization).
4) In addition, contingency plans should also contain a plan for how to handle communication with affected inhabitants that have got sensitive data stolen.
5) Internal communication regarding prioritization and ongoing follow-up of unresolved situations is very demanding, and over time the crisis management line can be short-circuited, and you would then need a good plan for how you want to handle this.
6) Training and exercising cyber-attacks are needed.
7) Cross-coordination (regulated) from local coordination (County general) and national authorities (National Security Authority) in such attacks sometimes creates confusion and uncertainty, and under the current regime planning must be done to be able to handle both.

The first 6 findings most relevant to the resilience and readiness in organizations are briefly discussed in the next sections. Finding 7 is only briefly incorporated in section 3.1.2, as the cross-coordination is an invariant property the organizations must relate to.

### 3.1.1 Cyber-attacks as separate risk and vulnerability assessment

Whether a good overall risk analysis of cyber-attacks would lead to a greater focus on measures and good contingency plans is uncertain anyway, especially considering that before this incident, one had not seen anything similar with the same consequences in other public organizations in Norway. Compared to a socio-technical approach (SBC-framework presented by Kowalski (1994)) to risk assessment, such a risk assessment only covers parts of what is recommended. This can be visualized as in figure 10.

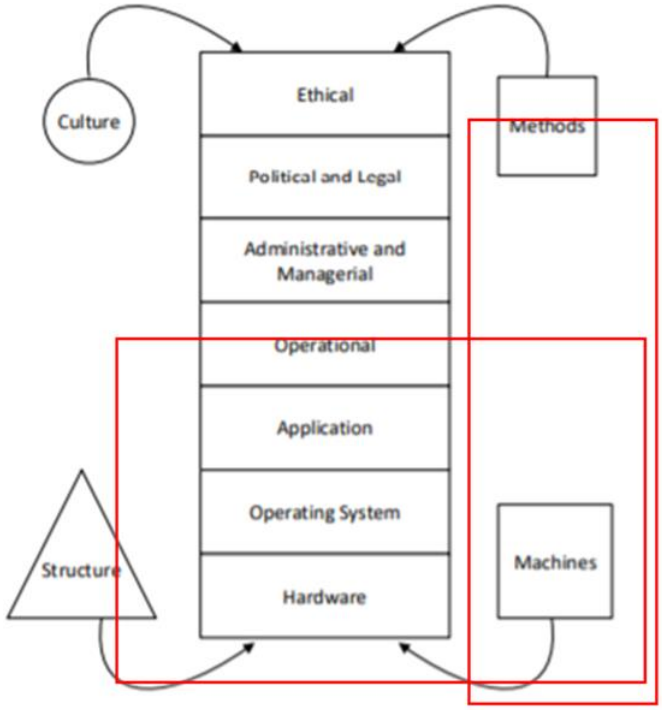



**Fig. 10.** Partial risk analysis (Østby & Kowalski, 2022c)

However, based on the findings, both from the questionnaire and the interviews, there was little knowledge of risk assessment of this type of attack. The consequences of not having carried out such a risk assessment, which is both recommended in the textbook for information security management (Whitman & Mattord, 2018) and mandated by national laws, regulations, and guidelines, were huge, and as the mayor of the municipality points out, "it is now important for elected officials to request reports on the risk work around cyber-attacks" (Østby & Kowalski, 2022c).

### 3.1.2 Information requirements

The need for information - and furthermore the pressure on the organization - is somewhat different than an incident with a cyber-attack. This can be visualized by a modified version of a "normal" information flow as presented in Østby & Katt (2019a) (publication 4), here presented with the "extraordinary" information pressure in red in figure 11.

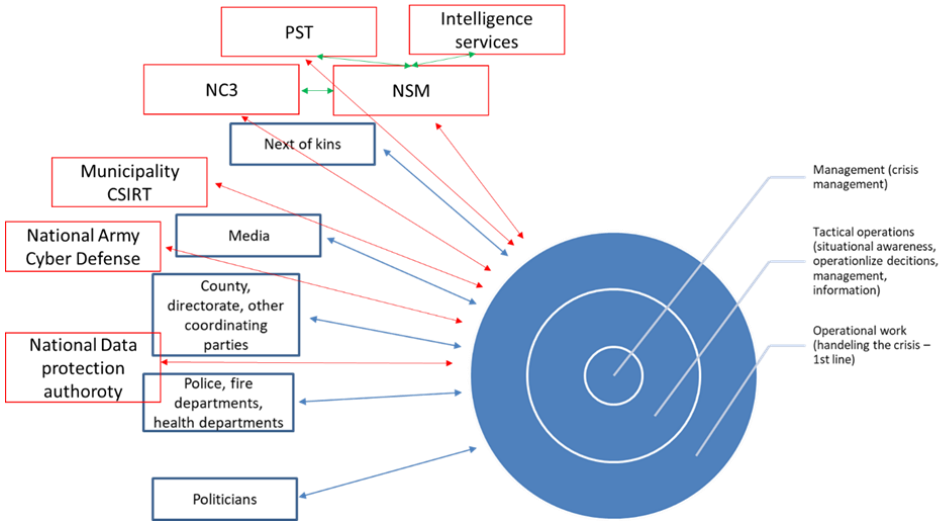



**Fig. 11.** Need for information sharing during cyber-attacks - modified (Østby & Katt, 2019a) (publication 4)

"Joint cyber coordination center (FCKS) consists of NSM, the Norwegian Intelligence Service, PST and Kripos (NC3), and is led by NSM." (Nasjonal Sikkerhetsmyndighet, 2017) But even though NSM has the coordination responsibility, the incident response team in Østre Toten was in dialogue with several of the units a number of times. To a large extent, this was about sending information to the authorities, and not receiving any information. Until, as the municipal director mentioned in the interview - that they required to be given access to a report that had been written.

### 3.1.3 ICT Incident Management and Recovery Team

Compared to the original model that Østby and Katt (2019a) (publication 4) proposed for the organization of crisis management of information and cybersecurity incidents and attacks on the tactical and operational level, there were no major deviations in relation to the type of work. But some aspects were done differently in the crisis management in Østre Toten, and in the beginning the experience of whether it was tactical work or operational work was rather fluid. Although the IT manager was initially alone in the crisis management, the ICT incident response manager also attended as soon as this person was pointed out (4 days after the incident). It was also the case that, firstly, crisis management by the municipal director, and secondly, tactical management by the ICT operations manager, and finally the operative teams all were in contact with the police and NC3. The ICT incident response manager was initially the leader of both tasks, and there were also two different experts from ATEA/KPMG to support the different work in the two teams. The ICT incident response manager left his position in Østre Toten during May 2021. The content is presented in figure 12.

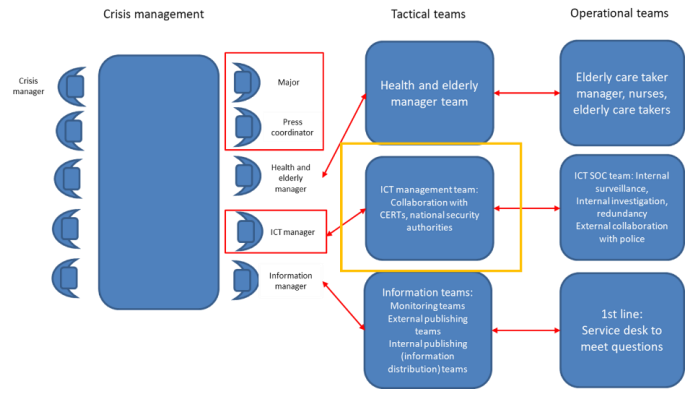
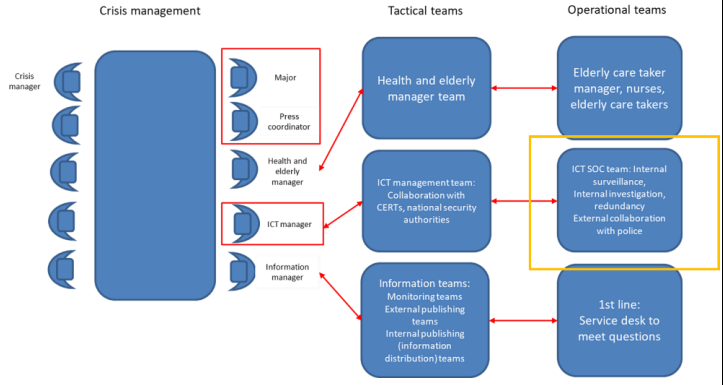
| | |
|---|---|
| Tactical Team:<br><br>ICT incident response manager (until June 2021)<br>Hired resource from Accenture (from June 2021)<br>Advisor from KPMG<br>IT manager (left the team when he was moved to IKOMM)<br>Finance manager |  |
| Operational team:<br><br>Also, ICT incident manager (until June 2021)<br>Recovery manager (from June 2021)<br>Security experts from first ATEA then KPMG<br>Recovery experts<br>Intelligence/interrogance experts |  |

**Fig. 12.** Participants in tactical and operational teams - explained (Østby & Katt, 2019a) (publication 4)

What is important to convey is that Østre Toten was not equipped with the personnel to cover this work, either at tactical or operational levels. For Østre Toten and other organizations, it is important to be able to prepare to get such teams in place in a similar crisis. Whether these are internal or external should be settled by the organizations themselves, but agreements should be made, and notification lists/lists of names created for the emergency planning system (Østby & Kowalski, 2022c).

### 3.1.4 Alert/notification team - sensitive personal data for sale on dark web

When the incident escalated with sensitive personal data being posted for sale on the dark web, a data protection officer was also brought into the crisis management. In order to handle the exchange of information with those affected (and possibly next of kin), an alert/notification team was set up. This is presented in figure 13.

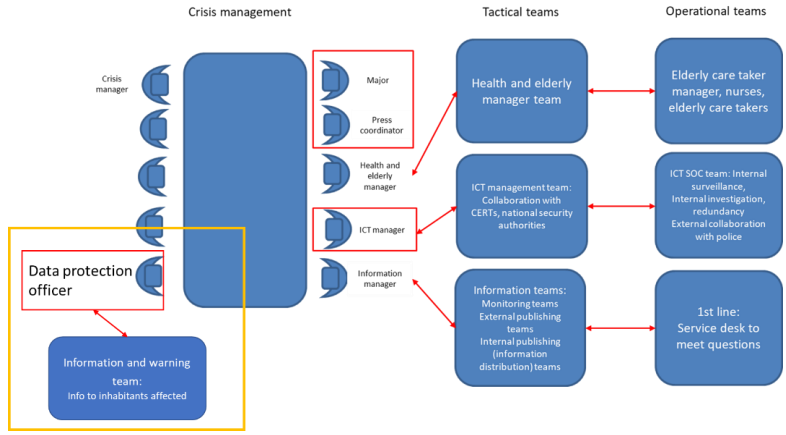
| | |
|---|---|
| Alert/notification team<br><br>Data protection officer<br>A person from adult education<br>A person who had previously led the psychosocial crisis team in Østre Toten<br>A communications consultant<br>Legal assistance from KPMG |  |

**Fig. 13.** Alert/notification team (Østby & Kowalski, 2022c) (appendix 1)

You do not necessarily know whether these are the exact right people for another organization, but the emergency plan should still include a description of tasks, as well as a notification list with necessary resources. The tasks that were carried out are well described in the results from the interview with the data protection officer (appendix 1).

### 3.1.5 Internal communication - crack in the crisis line (?)

Over time, it turned out that the crisis line from the crisis management generated a sense of fatigue in the organization. There was a kind of crack in the crisis management line, while at the same time there was more pressure on the operational ICT recovery team (see figure 14). However, to be able to have the direct dialogue with the operative team created optimism in the organization. It should be noted that the respondents indicated in their interviews that the operative team under the leadership of the recovery manager had clear guidelines/priorities from the strategic crisis management.

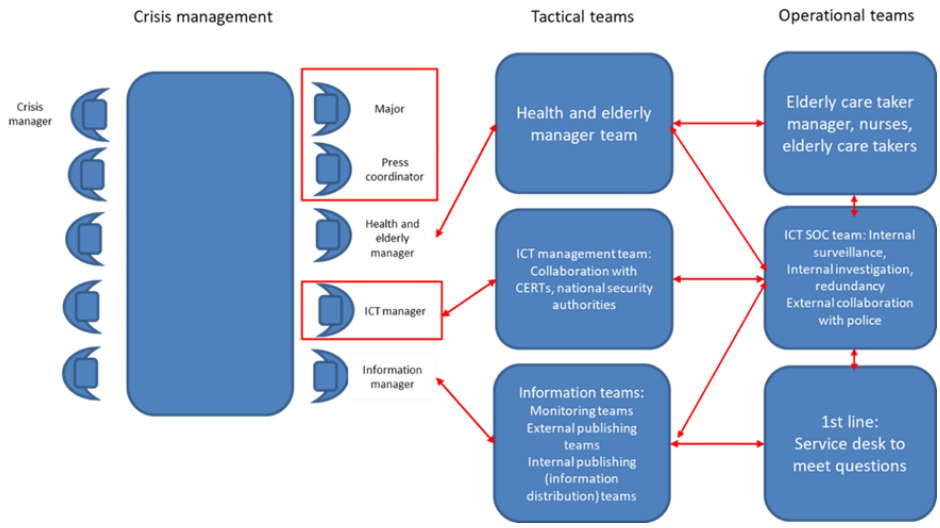



**Fig. 14.** New crisis management lines towards operational ICT team (Østby & Kowalski, 2022c)

Whether this is a good solution must be decided by any organization themselves, and resources must also be assessed in relation to it, but one should consider the pressure on the operational ICT recovery team in the sequence of events when this happens at some point. In addition, there should then be agreement and trust that this can work well for the entire organization. The recovery team should be informed in a timely manner about the current priorities of the strategic crisis management.

### 3.1.6 Training and exercises

The results from the questionnaire distributed in this case-study indicated that most of the respondents did not know that the organization had a security program. An information security program was described as "consisting of an organizational plan with tasks/functions that are needed, certification program, education, training, exercises etc." (Whitman & Mattord, 2018).

In the interviews, there was still a common understanding that such incidents must be trained and rehearsed. When asking the question about what they had learned from the attack, it often got a bit quiet, and it was not easy to analyze what the organization had learned from the attack from those answers. When asked a little more directly about contingency plans, however, some matters emerged more clearly, including the understanding of what a cyber-attack entails with the consequences in the organization - which must be dealt with.

An example is from the nursing home, where they had plans for power outages, and thus a list that had been updated 24 hours before the attack with an overview of patients and which medicines the individual should get. But, to get into the medicine cabinet, they had to use a card solution, which was then no longer active because of the attack. Other systems that were out of order were e.g., notifications/alarms for the residents, which led to the residents having to use manual bells. These examples should apply to other

organizations and can easily be entered into scenarios for exercises (Østby, Berg, et al., 2019) (publication 8).

## 3.2 Preparing for exercises as activity

In this section the preparation for exercises phase is discussed in regard to development from participatory action research analysis.

To prepare for information- and cybersecurity exercises, we have proposed and publicized the following artifact for information- and cybersecurity exercises consisting of

1) vulnerability analysis to identify risks from an overall perspective but also for the specific organization,
2) threat-assessments existing (and not existing) in the organizations,
3) plan and design a socio-technical scenario for the exercise,
4) plan for simulation that are realistic and based on the organization's maturity,
5) and finally, in terms of a crisis impact exercise; investigate the organization's responsibility (laws and regulations), crisis management roles and responsibilities, and continuity plans, to prepare for introductory lectures (Østby & Kowalski, 2020) (publication 6).

This type of preparation can be referred to as a user-centric approach, where you **identify the customer needs** before you specify the 1) context of use, 2) requirements, 3) produce design solutions, 4) evaluate designs, and finally 5) find a system satisfied. This approach can be visualized like in figure 15.

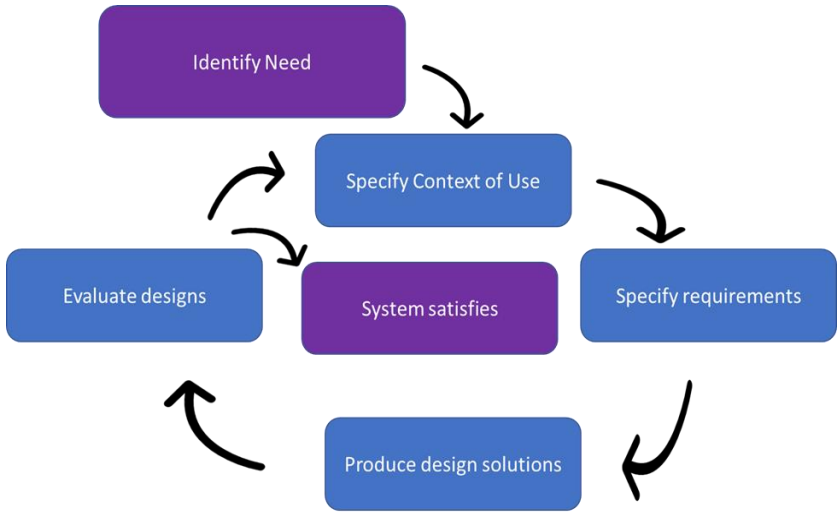
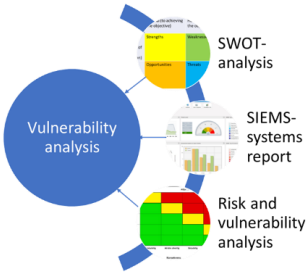


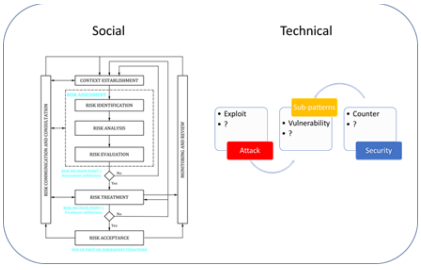

**Fig. 15.** User centric approach (Usability.gov, 2021)

In this section, participatory action research analysis (Kemmis et al., 2014) is presented based on the preparation for exercises framework (Østby & Kowalski, 2020) (publication 6)).




Towards the first full-scaled test-exercise, a historical cyber-attack from the Innlandet hospital trust was used and developed as a scenario. Already with access to risk- and vulnerability analysis from the hospital trust, and reports from Sykehuspartner from the last year, it was possible to do a SWOT-analysis to start to develop the learning goals for the exercise. At this stage we did not have access to any of Sykehuspartner's system risk assessments though, so we had to use the risk discovered from the previous attack as the foundation for creating the technical architecture and thereby also the attacks for the exercise. For the Ahus/Sykehuspartner exercise however, we got access to the risk-analysis of the three systems we chose to attack and were thereby able to write also the consequences for the social framework of the exercise.


Before the actual full-scaled exercise with Ahus and Sykehuspartner a test-exercise was executed. For the test-exercise, we only had access to national authorities' threat-assessments, but for the Ahus/Sykehuspartner exercise we had access to the South-Eastern, the Northern, the Central, and the Western Norwegian Regional Health Authorities threat assessment for 2022 (exempt from public disclosure) and were able to tune in on relevant measures from the assessment. For the test-exercise however, we had been given access to information from a previous attack at the Innlandet hospital trust, and such historical attacks are as mentioned in the publication also vital for threat assessments (Østby & Kowalski, 2020) (publication 6).




A part of preparing for exercises is to target these types of scenarios to the right type of exercise (Østby, Berg, et al., 2019) (publication 8). In the Norwegian Cyber Range community, it has been suggested that one should write the scenario first to prepare an exercise. We see that this only works for exercises at the lowest level of readiness and maturity (like the scenarios at ovelse.no) and moreover when you target a bigger group with a variety of participants (like in seminars or for large student-groups). Scenarios need to be developed over time, and especially for exercises involving an EXCON-team, the involvement and understanding of all the previously mentioned steps in this section is essential for the final scenario-result.

However, by taking part in developing and publishing ovelse.no, we have been able to establish Norwegian national online information security scenarios which can be used to train awareness and knowledge at an organizational responsibility level. ovelse.no (NSM et al., 2020), was established as a project within DSB's national exercise Digital2020 (DSB,

2020) for them to be able to provide exercises for a broader public audience than the main exercise. The project-work was a collaboration between NSM, DSB, The Digitalization directorate, NorSIS and NTNU, and relevant contacts have been established in the process. To develop the platform, the project group used DSB's exercise guidelines for discussion exercises. Then, based on the intention from Østby et. al. (Østby, Berg, et al., 2019) the different scenarios were analyzed based on socio-technical frameworks suitable for a discussion exercise. This is presented in figure 5 in publication 8 (Østby, Berg, et al., 2019). A questionnaire linked to each scenario is developed to see if what we analyzed was in line with how the users experience the scenarios (work in progress) (NSM et al., 2020). Twelve scenarios were developed based on the most known scenarios in Norway in 2020 (The Norwegian Business and Industry Security Council, 2020), and relevant discussion questions (and thereby some good advice) were developed to meet different sized organizations. Finally, the technical description with the desired user-approach and processes were developed.

In November 2022, more than 830 email-addresses from 513 organizations had been registered in ovelse.no. The variety of organizations is presented in table 7. The data variation is collected from The Brønnøysund registers based on the organization number registered when entering the web-platform.

**Table 7. ovelse.no users**

| Type of organization | Total number | 0 – 20 employees | 20 – 100 employees | 100+ employees |
|---|---|---|---|---|
| Corporation (aksjeselskap) | 175 | 48 | 41 | 86 |
| Public limited company (almennaksjeselskap) | 6 | | 1 | 5 |
| Other legal entity (annen lovlig enhet) | 3 | | 2 | 1 |
| Other companies in relation to separate law (annet foretak ift. særskilt lov) | 24 | | 3 | 21 |
| Responsible company with shared responsibility (Ansvarlig selskap med delt ansvar) | 1 | | | 1 |
| Housing association (Boligbyggelag) | 1 | | | 1 |
| Sole proprietorship (Enkeltpersonforetak) | 23 | 22 | | 1 |
| Association/team/facility (Forening/lag/innretning) | 18 | 8 | 3 | 7 |
| County municipal enterprise (Fylkeskommunalt foretak) | 1 | | | 1 |
| County municipality (Fylkeskommune) | 9 | | | 9 |
| Intermunicipal company (Interkommunalt selskap) | 7 | 1 | 1 | 5 |
| Municipality (kommune) | 81 | 7 | 7 | 67 |
| Norwegian registered foreign company (norsk-registrert utenlandsk selskap) | 1 | | | 1 |
| Organization link (organisasjonsledd – typisk statsforvaltningen) | 113 | 2 | 23 | 88 |
| Cooperatives (samvirkeforetak) | 2 | | | 2 |
| Savings bank (sparebank) | 3 | | | 3 |
| Govern (staten) | 14 | | | 14 |
| State enteprise (statsforetak) | 4 | | | 4 |
| Foundation (stiftelse) | 2 | | | 2 |
| Unknown | 4 | | | 4 |
| Sub-unit for entrepreneurs and public administration (underenhet til næringsdrivende og offentlig forvaltning) | 4 | | | 4 |

The presumption that these types of scenarios also will work for students, led to two such scenarios were developed to meet the learning goals in the IMT-4115 Introduction to information security management (NTNU, 2021) exercise (Østby & Kowalski, 2022b) (publication 3). In comparison with the ovelse.no scenarios, the two student-exercises

scenarios were developed to meet the management-aspect of the course, and to support learning activities/deliveries. One example is that the students were delivered the information security policy from the fictive organization in the scenario. Another example was news-articles.

A scenario can also be developed from a policy point of view. In the preparations for a policy exercise in June 2022 (see CCIS exercise in table 11 below), the scenario was developed to be able to discuss challenges in today's regulations, not only in Norway but also internationally, and how this impacts information security in vital societal functions.

For the full-scaled test-exercise the scenario was developed to meet both socio-and technical needs based on the knowledge gained in the vulnerability analysis and most essential from an actual historical attack against Innlandet hospital trust. An architecture-setup based on how it was before the attack, and thereby the necessary systems were set up to meet the overall scenario. This can briefly be presented as in figure 16.

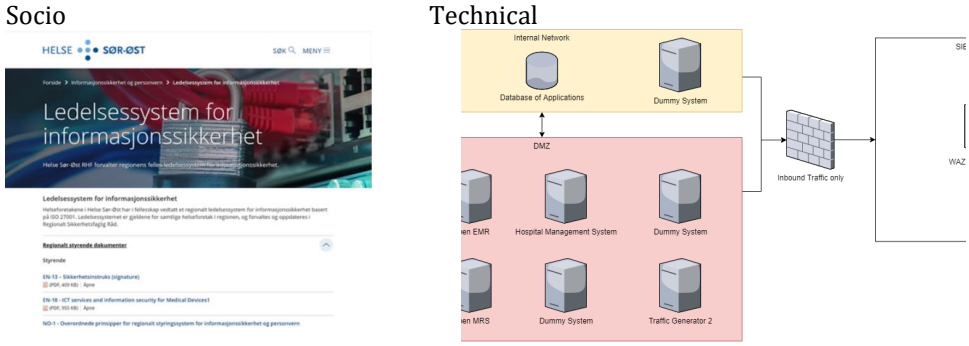
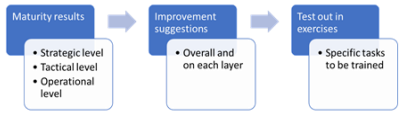



**Fig. 16.** Details from a socio-technical scenario

One must never forget though, that a little bit of imagination and capability (/cognition (Comfort, 2007)) to see patterns and how different aspects of future risks can give consequences and to bring this forward into scenarios for exercises, is beneficial.




To target a better suited learning environment for the organization at hand, one may use EMM's to see if there are any issues as presented in figure 4, or one may use it as a starting point for discussions for a step-by-step implementation plan for information security (Østby et al., 2020) (publication 6) In the full-scaled test exercise we tested out the first assumption (created learning activities to push reporting), and we had a master-student to observe and interview the "head of SOC" and the "ICT manager (also CISO)" after the exercise about how they experienced these targeted learning activities.

> "According to the contingency plan, the CERT has a responsibility to contact external parties outside the organization, such as the police, NorCERT and HelseCERT. Both the user that worked with the SIEM system during the exercise and the person playing the role as the chief information security

> officer addressed the issue that there was lack of some form of communication to log what was done at CERT. This is a clear contrast to what goes on in the emergency team, where everything they do is constantly logged into the CIM system. That means that everyone has the opportunity to see what has been done and just as importantly, after the crisis you can use these logs to find areas for improvement and evaluate what went well with the crisis management and what can be done better the next time." (Huseby, 2021)

A note to the "use these logs to find areas for improvement and evaluate" found in the test-exercise that Huseby is referring to (Huseby, 2021), is that in the exercise with Ahus/Sykehuspartner we were introduced to the fact that they have a system for evaluation- and improvement they use after both incidents and exercises. They systematically log learning points during and after exercises and moreover close the issues one by one as a deviation- and action to improve the process. This is in line with what we suggested in Østby et al. (2020) (publication 2), a process to systematically close the socio-technical gap. Our suggested improvement-process is presented in figure 17.


**Fig. 17.** Maturity improvement process (Østby et al., 2020) (publication 2)

The targeted learning activities in the test-exercise were to request information, of which the management-team would further need to ask the CERT for information. Moreover, targeted learning activities also covered the need for decisions at the CERT. Huseby's (2021) observation made it clear that these learning activities were able to raise awareness about the issues at hand:

> "During the exercise, the chief information security officer pointed out the lack of having control on what was done at CERT and if they were having any new information. That led to several phone calls with the purpose of getting updates on the current situation and to know who the CERT had contacted." (Huseby, 2021)

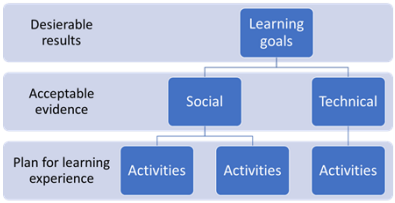
---

> ""I wish to have information on what is done at the SIEM " – Chief information security officer, full-stack exercise at Norwegian Cyber Range" (Huseby, 2021)

Moreover, the request for information to CERT as a learning activity also had awareness content to the participants:

> ""To coordinate all the sharing of information by phone, interrupted my work" - SIEM worker, full-stack exercise at Norwegian Cyber Range" (Huseby, 2021)

The idea of integrated SIEM-information into the CIM-system is still considered, but more research is needed to establish the balance between the "right" information needed from the management team and the "right" information to share from the CERT. That is, what would be the accepted level of information as presented in Østby et al. (2020) (publication 6).




A final part of the preparations for the exercise is lectures beforehand the execution. What type of lectures one would need is also dependent on the type of exercise you execute. In Østby & Kowalski (2020) (publication 6), we suggest a socio-technical backward design model (Yale, 2019), modified to consider both socio and technical aspects in the learning goals. Our suggestion is that lectures should be such activities when necessary. For the table-top exercise with the IT-management-group at NTNU, and for both the full-scaled exercises (test-exercise and Ahus/Sykehuspartner), four different lectures were executed. These were (Østby & Kowalski, 2020) (publication 6):

1) Regulations in security and emergency at xx organization (laws, regulations, and guidance's), and other tasks crises management should be prepared for.
2) Crisis management and work in crisis staff: Situational analysis, need of resources (personnel and material), roles in crises and operative management.
3) Information in emergencies, crisis management brief, crises communication and CIM.
4) Emergency plans, task lists for roles in crisis (critical analysis of the team's emergency plan).

The first lecture is an outline on what is required in the specific organization. As mentioned, laws, regulations, and guidance's, but also information security in letters of allocation[2], and the written strategies and policies for the organization. The second lecture is more of a traditional lecture on crisis management, but for some organizations it is needed to adapt and/or modify the lecture to the theories used in the specific organization. E.g., for the Ahus/Sykehuspartner exercise, we used facets from Lunde (2019) to meet what the health-sector in Norway "use" on a daily basis. The third lecture is about how to share and collect information, but also about how to relate to the media. The last lecture is a review of the organizations' risk-and vulnerability plans, contingency plans, and crisis management plans, and thereby comments on what is missing towards a cyber-attack.

When asked about how they found the lectures relevant, the ICT-management team at NTNU answered as presented in table 8 (6 respondents), and the management team at Ahus as presented in table 9 (7 respondents).

[2] Letters of allocations in Norway would be e.g., 'tildelingsbrev', 'oppdragsbrev' and similar.

**Table 8. Relevance of lectures beforehand exercises ICT-management team at NTNU (Østby & Kowalski, 2020)**

| | No relevance | Some relevance | Relevant | Very relevant | Huge relevance |
|---|---|---|---|---|---|
| Regulations in security and emergency at Universities and Colleges (laws, regulations, and guidance's), and other tasks crises management should be prepared for. | 0% | 16,7% | 50% | 16,7% | 16,7% |
| Crisis management and work in crisis staff: Situational analysis, need of resources (personnel and material), roles in crises and operative management. | 0% | 0% | 33,3% | 50% | 16,7% |
| Information in emergencies, crisis management brief, crises communication and CIM. | 0% | 0% | 16,7% | 66,7% | 16,7% |
| Emergency plans, task lists for roles in crisis (critical analysis of the team's emergency plan). | 0% | 0% | 33,3% | 50% | 16,7% |

**Table 9. Relevance of lectures beforehand exercises Ahus**

| | No relevance | Some relevance | Relevant | Very relevant | Huge relevance |
|---|---|---|---|---|---|
| Regulations in security and emergency at Universities and Colleges (laws, regulations and guidance's), and other tasks crises management should be prepared for. | 0 % | 71,4 % | 0 % | 14,3 % | 14,3 % |
| Crisis management and work in crisis staff: Situational analysis, need of recourses (personnel and material), roles in crises and operative management. | 14,3 % | 57,1 % | 0 % | 14,3 % | 14,3 % |
| Information in emergencies, crisis management brief, crises communication and CIM. | 14,3 % | 57,1 % | 28,6 % | 0 % | 0 % |
| Emergency plans, task lists for roles in crisis (critical analysis of the team's emergency plan). | 14,3 % | 57,1 % | 14,3 % | 14,3 % | 0 % |

For the student-exercises, the first and last lecture were taken out as those are very much targeting a specific organization. How the students found the lectures relevant is presented in table 10 (51 and 11 respondents' year 1, 77 and 8 respondents' year 2).

**Table 10. Relevance of lectures beforehand exercise, student-exercise (Østby & Kowalski, 2022b)**

| | No relevance | Some relevance | Relevant | Very relevant | Huge relevance |
|---|---|---|---|---|---|
| Year 1, day 1 Crisis management | 3,9% | 11,8% | 58,8% | 21,6% | 7,8% |
| Year 1, day 1 Logs and information sharing | 3,9% | 19,6% | 56,9% | 19,6% | 3,9% |
| Year 1, day 2 Crisis management | 0% | 9,1% | 27,3% | 54,5% | 18,2% |
| Year 1, day 2 Logs and information sharing | 0% | 27,3% | 54,5% | 27,3% | 0% |
| Year 2, day 1 Crisis management | 3,9% | 16,9% | 45,5% | 23,4% | 7,8% |
| Year 2, day 1 Logs and information sharing | 6,5% | 19,5% | 44,2% | 23,4% | 3,9% |
| Year 2, day 2 Crisis management | 0% | 0% | 75% | 25% | 0% |
| Year 2, day 2 Logs and information sharing | 0% | 12,5% | 62,5% | 25% | 0% |

How many of the students who actually attended the lectures out of the answers in this question is unknown, since the lecture was recorded and could be watched outside the designated time. The results from the two other tables (5 and 6) are, however, from attendances, but only half of the attendances from Ahus/Sykehuspartner answered the survey. What we can assume from the answers is however that those who have experience with crisis-management work like at Ahus, do not find the lectures as relevant

as e.g., the ICT-management team at NTNU. Results and experiences from evaluation of these types of lectures for crisis-management teams from municipalities, were on the other hand never scored as “no relevance” or “some relevance”.

## 3.3 Arranging and participating in games and executing exercises

Types of exercises are described in many templates (DSB, 2016a, 2016d, 2016b, 2016c; ENISA, 2009a; HSEEP, 2006), and research indicates exercises can support the improvement to reach relevant learning goals and transformational change. Being affected by Covid19, the number of exercises executed in this project were limited to participate in 9 exercises and run (in collaboration with others) 11 exercises, for a total of 20 exercises. In addition, the project supported the mentioned ovelse.no which was launched in 2020. An overview of the exercises is presented in table 11.

**Table 11. Participation in and execution of exercises**

| | Seminars | Discussion exercises | Games | Table-top exercises | Functional exercises | Full-scaled exercises |
|---|---|---|---|---|---|---|
| **Gatherings/participation in exercises** | Security divas 2022<br><br>Totalforsvarets cybersikkerhetskonferanse 2022<br><br>NorSIS seminar 2022<br><br>Cybercation, Estland, 2022<br><br>LEAN forum annual conference 2022 | Atlantic council 9/12 cyber security challenge (participant 2019, coach 2020, judge 2021 and 2022) | CS-Technopoly, Sikkerhetsfestivalen 2022 | | | |
| **Organizations** | | ovelse.no launched in 2020<br><br>Partner conference CCIS 2022<br><br>Discussion exercise LEAN-conference 2022 | | ICT-management group at NTNU 2019<br><br>Management group Kripos 2022 | SIKT/Øvelse Morris 2022 | Ahus and Sykehuspartner 2022 |
| **Students** | | Annual student-exercise Introduction to information security management, master class course 2020 - 2022 | Lillehammer Megagame 2019 | | | Test-exercise 2021 |

If the preparation for exercises presents a readiness and maturity at a low level, then it may be appropriate to start with simple seminars/training or discussion exercises, while at a high level of readiness and maturity you can arrange functional exercises and full-scale exercises. Different types of activities and exercises for such training are presented in figure 18 (HSEEP, 2006), and there are also good guides for exercises at the Directorate for Community Security and Preparedness (DSB) (DSB, 2016) and at The European Union Agency for Cybersecurity (ENISA) (ENISA, 2009).

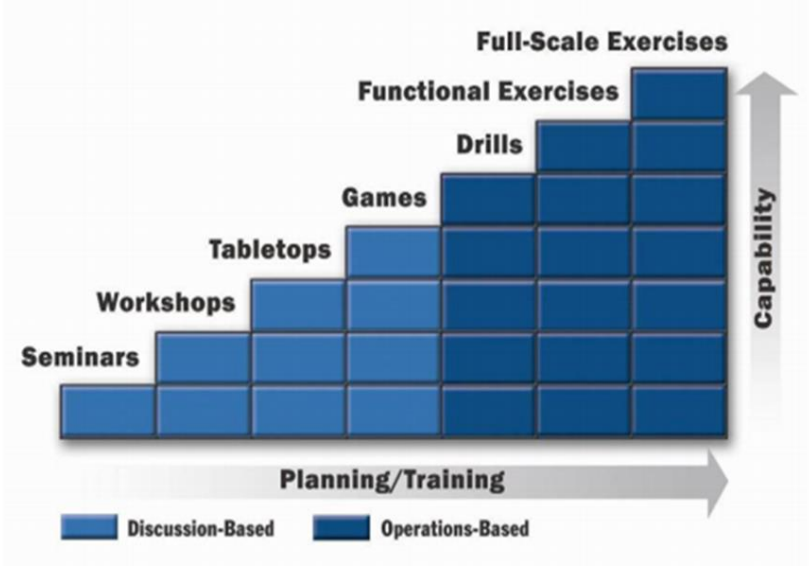



**Fig. 18.** Different types of exercises (HSEEP, 2006)

Gurnani et al. (2014) and Omiya & Kadobyashi (2019) suggest exercises to be divided into two groups – discussion-based exercises and operation-based exercises. This is also visualized in the HSEEP model (figure 11) by the different shades of blue. It is not necessary however, that one would stop discussing in the operation-based exercises. We did however experience such "split" in the Ahus/Sykehuspartner exercise, as we were not able to instruct/guide the CERT-team at the right stages in the scenario. An output solution from the participatory action analysis from this exercise is presented in the Exercises for organizations section below.

In the following two sections student exercises and participation in games are briefly presented and discussed, and relevant outputs from exercises from organizations are outlined.

### 3.3.1 Student exercises and participation in games

A variety of student-exercises within information- and cybersecurity is executed in different universities. This is either as capture-the-flag (CTF) or red-team – blue-team exercises, often with the context of adversarial thinking as the learning goal. In addition, Games are part of everyday life. Americans spent over $25 billion on video games in 2010 (Muntean, 2011), and have increased to $60.4 Billion in 2021 (Entertainment software association, 2022). One sees a rise in games also used in student courses (Hainey et al., 2011; Koutromanos et al., 2015), and recent studies also present that information security is no exception (Mostafa & Faragallah, 2019). Studies also present incident response exercises for management courses (Grimaila, 2004; Østby & Kowalski, 2022b) (publication 3), and in this section some of the experiences related to introducing two types of exercises in the information security track at NTNU for students is presented.

In Østby & Kowalski (2022a) we suggest introducing a management course where the students should not only take part in lectures and learn about game-theories but build and execute a serious game themselves. The suggestion emerged after experiences from participating, coaching and judging in the Atlantic council 9/12 cyber security challenge (Atlantic_Council, 2021), and also arranging a megagame on behalf of NTNU (Sikkerhetsfestivalen, 2019). Given the possibility of learning the European structure for response to information- and cybersecurity threats through the competition as a participant, and as a coach to be able to see how the students were able to both seek and grasp information in a short amount of time in this type of exercise, we found that a course with the same elements would be beneficial for the students. From these activities being extra-curriculum activities, the idea for a management course to adapt these learning-activities into an academic format, the NTNU requirements to build such a course (NTNU, 2019a, 2019b) were used to suggest such a course.

Information security being multi-disciplinary in nature, "1) critical theory and socio-technical approaches to create scenarios from the information security landscape, 2) social learning, and 3) sustainable goals for information security" was suggested as the content of the learning outcome (Østby & Kowalski, 2022a) (publication 5). All these three variables are vast in scope, and therefore we suggest that a variety of games could be developed, as presented in figure 19.

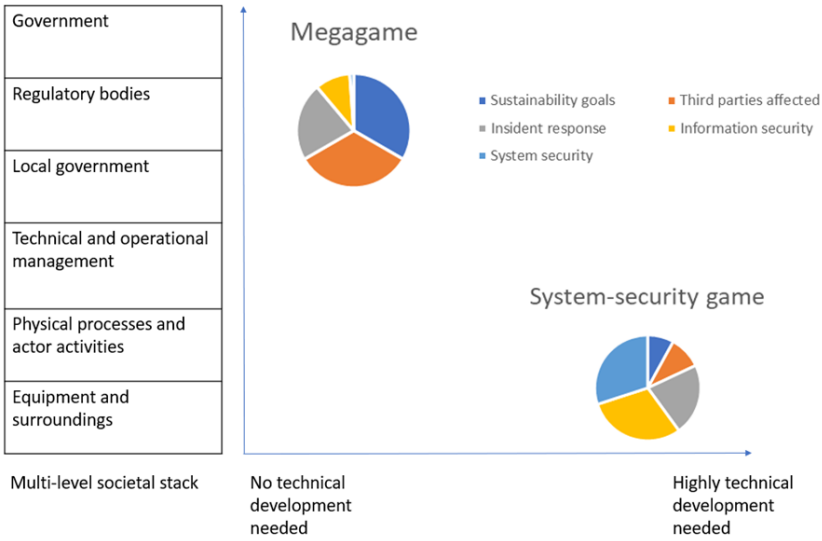



**Fig. 19.** Scoping development of serious games in information- and cyber security incident response in a master study course (Østby & Kowalski, 2022a) (publication 5)

The course is not yet introduced, but as generation Z and generation Alpha growing up with games will enter the universities, they would be likely to learn better from such games.

In 2021, we introduced a crisis management exercise in the IMT 4115 Introduction to Information security management course (NTNU, 2021). An evaluation survey was executed among the students, and adjustments were implemented in the 2021 course.

The results presented in Østby & Kowalski (2022b) (publication 3), shows that learning goals from a triple-loop learning context with proper hotwash and evaluation sessions, were met to a great extent. This is presented in figure 20.

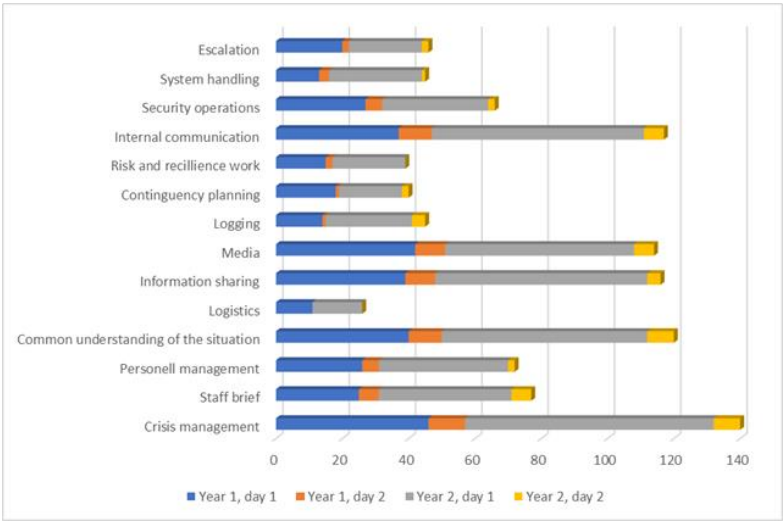



**Fig. 20.** Factors in the scenario the students scored as achieved (Østby & Kowalski, 2022b) (publication 3)

A course for serious games as presented in Østby & Kowalski (2022a) would therefore also benefit from a triple-loop-learning environment, and such should be a relevant factor in the course when implementing it. The triple-loop-learning we suggested in the crisis management exercise in the IMT 4115 course is presented in figure 21.

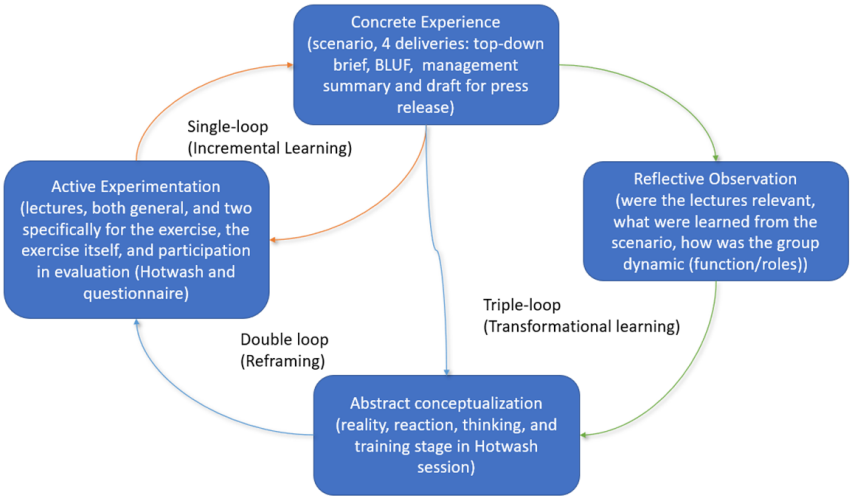
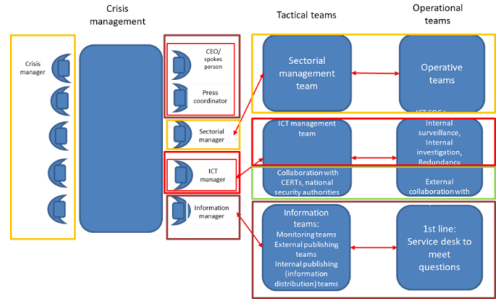



**Fig. 21.** Pathways of and outcomes of single-, double- and triple-loop learning adapted from Medema (Medema et al., 2014; Østby & Kowalski, 2022b) (publication 3)

Finally, to meet the expectation of organizational learning from these types of environments, we also tested this type of learning activities for the Ahus/Sykehuspartner exercise, which will be presented in the next section.

### 3.3.2 Exercises for organizations

When it comes to more advanced exercises such as functional exercises and full-scale exercises for organizations, we firstly recommend preparing exercises by acquiring a good overview of the organization which will be trained (Østby & Kowalski, 2020) (publication 6). Next, we suggest creating a good exercise directive with exercise goals and thereby activities led by the instructors in the white team. Finally, we suggest writing a scenario based on the readiness and maturity levels in the organization to be able to give a sense of mastering the tasks at hand. To carry out the exercise, we have suggested a teaching artifact for EXCON teams for exercising the organization (Østby, Lovell, et al., 2019) (publication 7).




The variety in "who should be trained" (Østby, Lovell, et al., 2019) (publication 7), are in our opinion the baseline for how one builds up an EXCON-team. The example we used in the publication (publication 7), is a municipality, but it could as well have been an oil-company. It is important that one firstly would figure out who one would train and what type of personnel you need to train that team or organization. At the time when examples were presented from the Østre Toten case study in the lectures for the Ahus management group (Østby & Kowalski, 2022c) (believing the content was of general interest), I got some reactions that the examples should have been more targeted towards them. Which really should not have come as a surprise to me, as the whole idea behind "who should be trained" is to provide the best targeted trainers (in that case myself as an instructor/on the white team). The results from how the Ahus management team answered to the triple-loop-learning evaluation was however interesting, as the targeted learning objectives also in that case were all in line with the plans adapted in both the instructions/lectures and in the scenario. These results are presented in figure 22. One example is that logistics were never a part of the learning goals, and so were not intelligence (for the management team).

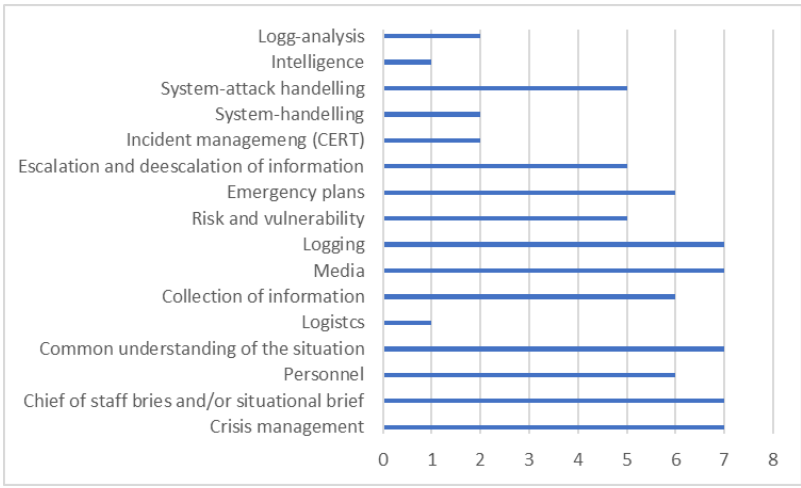
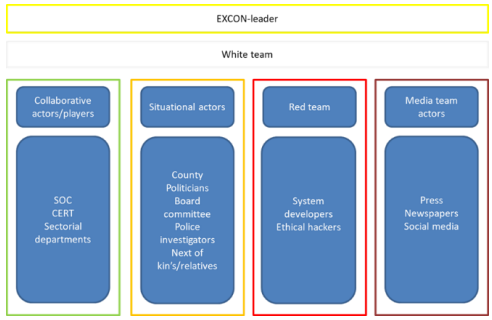



**Fig. 22.** Targeted learning objectives met




For the Ahus/Sykehuspartner exercise itself however, a long process of getting volunteers to be in the EXCON-team was executed. And for both the test-exercise and for the Ahus/Sykehuspartner exercise, the suggested EXCON-team artifact in Østby, Lovell et al. (2019) (publication 7) were followed. In both the test-exercise and in the Ahus/Sykehuspartner exercise however, we were not able to get good communications between the red-team and the rest of the EXCON-team, and moreover between the red-team and the instructor for the operational team (SOC/CERT). Running scenarios in these two communities we are trying to merge is new and perhaps a bit ground-breaking, and we were not prepared for a collaboration in a stream-lined scenario with learning goals. To meet the challenges, the final output from the participatory action research analysis is for the exercise control to collaborate based on first of all presence in the EXCON-team, but also a plan for communication between the EXCON-team and the instructors. Specially to meet the scenario timeline. This means that e.g., when it is time to move forward in the scenario, the instructors (white team), needs a dialogue with the red team (or later on in the scenario - with the EXCON-leader), to teach (help) the SOC/CERT overcome obstacles at hand. Otherwise, one will not learn, and a split as we experienced in the Ahus/Sykehuspartner exercise may occur, and suddenly two different scenarios will be the case, and very difficult to handle. Communication between the other instructors and also the EXCON-leader to collaborate with the instructors for strategic and tactical teams is also important. Then one would be able to recognize when the appropriate time to introduce learning activities according to the scenario timeline would be. In a dynamic scenario, it would be beneficial to have an open lead on this, but as mentioned – some learning activities must be scheduled fixed. A schematic model to deal with the above-mentioned problem is presented in figure 23.

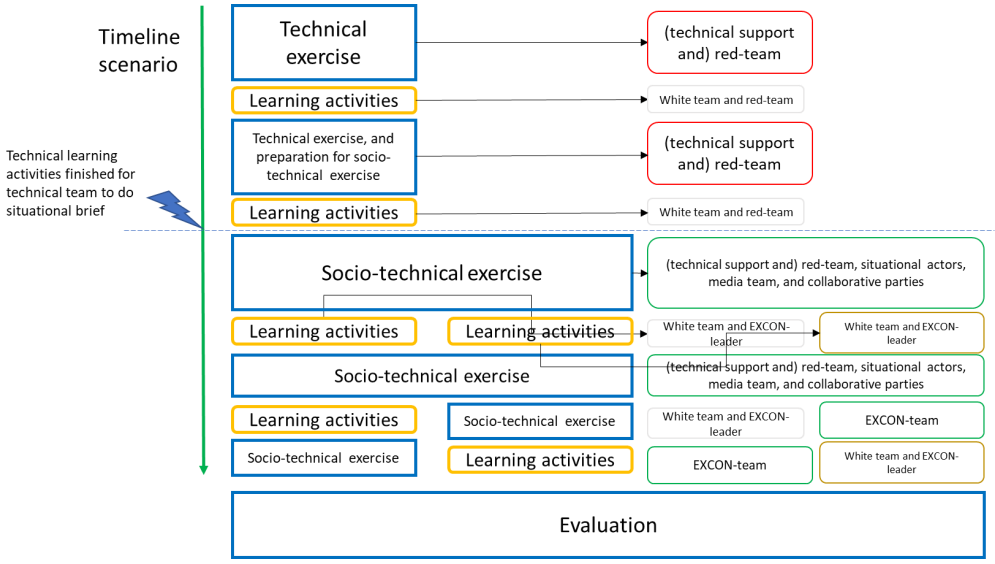



**Fig. 23.** Coordinated learning activities to meet the timeline of a scenario

To create a foundation for the exercise technically (to the technical team to discover the attack), we prepared for the technical/operational team to start the exercise ahead of the rest of the organization. The technical/operational team would also get a deadline to present a situational brief for the rest of the organization at a set time - marked with a stippled blue line in figure 23. Therefore, communication and learning activities to overcome obstacles before this set deadline would be essential.

It is also important to highlight the important role of the EXCON-leader. To be able to communicate in "ordered" forms and not overly disturb the exercise in progress, it is important that there are as few communication channels between the instructors and the EXCON-team as possible. Experiences especially from the Ahus/Sykehuspartner exercise showed that the instructors spent too little time with "their" teams. This issue is also pointed out in figure 23 by emphasizing the EXCON-leader as the main contact for the white team.

In the SIKT/Exercise Morris (NTNU, 2022) the exercise goal was to train information sharing between different SOC/CERT-teams, and a different EXCON-team was set up to meet a different timeline and scenario. The concept of 1) who are we going to train, and 2) what personnel do we need to be able to train was used to set up the team for the exercise. In the exercises we have arranged which involves both technical/operational, tactical, and strategic teams from organizations, the concept from Østby et. al (2019a) as a foundation to prepare a well-structured EXCON-team is recommended as long as the learning activities are coordinated as suggested in figure 23.

# 4 Rigor and relevance

Figure 24 below outlines a framework for research in information systems research that can be used to model the literature review process used in this research work. As the research has had an inductive approach, the relevance and thereby the needs in the society, and more specifically the resilience and readiness in public emergency organizations, were targeted firstly. Ideas were suggested, and case-studies, and exercises were planned. As we moved forward, the necessity of a more rigorous approach to validate the work was necessary. There was also a need for rigorous studies of academic theories, frameworks, and available instruments with methods as presented in (Hevner et al., 2004).

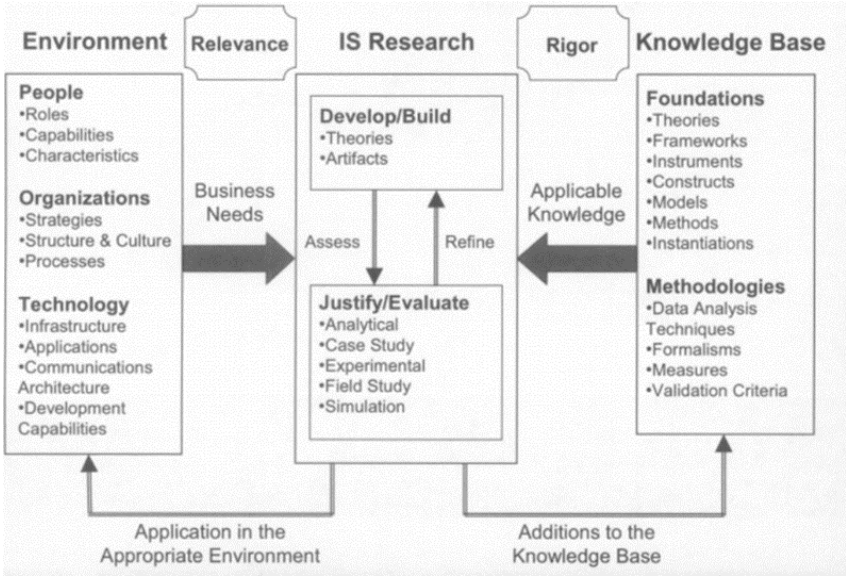



**Fig. 24.** Information systems research framework (Hevner et al., 2004)

Theories and frameworks of learning knowledge process (societal learning, organizational learning, institutional learning, and micro learning) and learning frameworks (game-loop-learning and triple-loop-learning) were applied in the research work to validate more rigorously the suggested learning artifacts. It was also important to execute a literature review to find applicable knowledge from previous studies in the area.

## 4.1 Frameworks of learning knowledge and learning frameworks

To distinguish between adaptive change and transformative change to crises in a society, it is suggested that adaptive change

> "remains largely within the reigning paradigm and structural context set by the formal policy process"

and that transformative change

> "influence triple-loop-learning phases of a policy cycle in which problems are framed, strategic goals are set, and policy is formulated." (Pahl-Wostl et al., 2013)

To deal with the policy challenge by the general trend of technological determinism in regard to public sector services, we have suggested to use triple-loop-learning measures for a diversity of learning methods from 1) organizational learning and therein management learning, 2) institutional learning, and 3) microlearning. One would also need to adapt both socio- and technical measurements for all learning goals to meet the socio-technical gap (Østby et al., 2020).

In Østby et. al. (2020) (publication 2) we suggested a step-by-step framework to choose the right learning methods for the different socio- and technical (S and T in the figure) learning goals. The suggested framework is presented in figure 25.

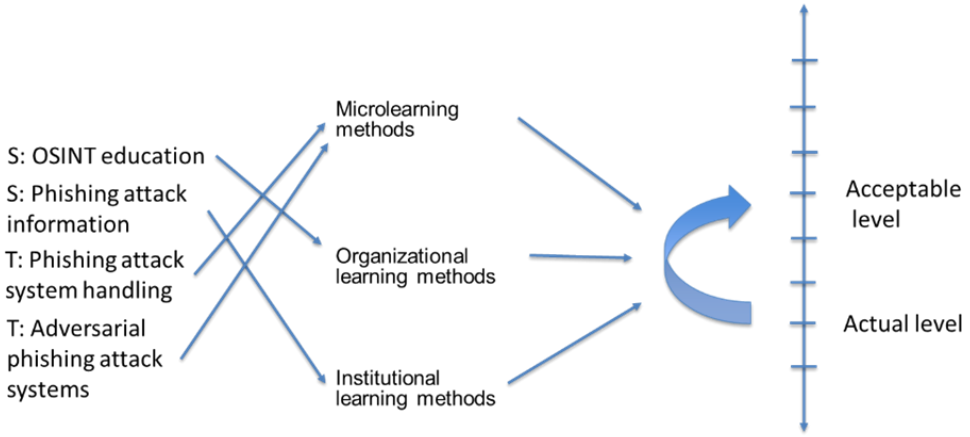



**Fig. 25.** Implement processes to learn action points (Østby et al., 2020)

The framework is based on what level of maturity and readiness is measured in the organization ('Actual level'), and how to get to an 'Acceptable level' needed and afforded. In such a context, management and training is essential to step up the levels (Østby & Kowalski, 2022b).

A crucial management responsibility during a crisis is to make decisions. However, "In reality, crisis-response efforts depend on many people in several networks" (Boin & Hart, 2001). Relations to management responsibilities would be that

> "decision making theories (Parmigiani & Inoue, 2009) are transferable to crisis management in both emergency organizations (Lunde, 2019) and in information security incident response." (Scarfone et al., 2008)

Being dependent on the organization to adapt to leadership and training, the organizational learning culture is suggested to be vital to the transformation (Xie, 2019).

> "Transformational leadership elevates mutual interests among employees and motivates followers toward a shared vision." (Bass, 2000)

In Xie's literature review on "how relationship between leadership and organizational learning culture (OLC)/learning organization (LO)/organizational learning (OL) is measured in the literature" (Xie, 2019), he found that "transformational leadership has been more frequently studied than other types of leadership in recent years", and that "compared with transactional leadership (supervision, organization, and performance), transformational leadership is more likely to bring the most potential out of the employees", even though some studies suggests the opposite (Xie, 2019). Information and system security is most often not the main area of product or service in an organization, and to adapt to the needed organizational changes transformational leadership is needed.

In complex organizations where system security is outsourced (e.g., to an external SOC/CSIRT), and thereby not necessary as a part of the learning culture in the organization, microlearning methods might be needed.

> "Leaders need to understand the patterns of complexity and learn to manipulate the situations of complexity more than its results." (Marion & Uhl-Bien, 2001)

And, as Marion & Uhl-Bien suggested in 2001, "transformational leadership literature begins to address such behavior." (Marion & Uhl-Bien, 2001) They recommend enabling rather than controlling network dynamics and call it complex leadership. After a number of years running crisis management exercises and training, it is found that time for participants to reflect and come up with their own suggestions to transform needed changes is essential in any stage of a step-by-step improvement work as presented in figure 10. In addition, a collaboration in the preparation for exercises to understand the level of maturity is needed (Østby & Kowalski, 2020).

In the context of information security being transdisciplinary in nature, one must also consider the diversity amongst the different institutions in need of change. Institutional learning and change (ILAC) can be referred to as

> "a process which can change behavior and improve performance by reflecting on and reframing the lessons learned during the research process." (Watts et al., 2007)

Thereby, both research institutions and other institutions must reflect and reframe the lessons considering new inputs from studies. Such changes from research can be adapted to organizational learning (Østby & Kowalski, 2022b) and support further transformational leadership.

> "The global availability of cyberspace objects has created the problem of ensuring the stable operation of modern production under random and targeted cyber-attacks that lead to long-term and difficult-to detect effects on the process control, which can result in catastrophic consequences." (Zegzhda, 2016)

The sustainability of such systems is therefore required, and sustainable learning in organizations must be considered.

> "A sustainable learning organization would be an organization that has enough sustainability knowledge and acts accordingly, and that may be considered as a role model to prevent, eliminate and/or reduce the environmental and occupational risks associated to their operations while enhancing and strengthening its profitability." (Velazquez et al., 2011)

In Østby & Kowalski (2022a) we suggest sustainability as a required part of creating games for learning information security, and one may argue that learning system-security sustainability through other exercises can be adopted through well-developed scenarios. As would be the responsibility of transformational leadership in preparing for and executing exercises (Østby, Lovell, et al., 2019; Østby & Kowalski, 2020).

## 4.2 Review of literature on information security management in public organizations

Critical tasks decision makers need to accomplish in crisis' is presented by many researchers (Lalonde & Roux-dufort, 2013), and exercises to learn necessary tools to manage the tasks and get awareness of own reactions in stressful situations are suggested for student exercises to understand how difficult a crisis is to manage (Lalonde & Roux-dufort, 2013).

This is transferable to complex organizations struggling to understand the overwhelming crisis that can occur, and a variety of training and exercises based on what maturity level the organization is at is needed (Østby et al., 2020). Especially in the emerging landscape of information- and cyber security incidents and attacks. In this section we present current research on information- and cyber security management and crisis management exercises.

As no scientific publications met the expected results of "information- and cyber security crisis management exercises in public emergency organizations", the search-string criterions were developed to meet both "information-and cybersecurity" exercises in general and more specific "management exercises", and the limitation of "public emergency organizations" were excluded from the search strings to broaden the search. The search string criterions used is presented in table 12.

**Table 12. Search string criterions**

| Criteria | Search goals and search strings |
|---|---|
| Primary search terms (PST) | information security management exercises, cyber security management exercises, management exercises in information security, management exercises in cyber security, information security exercises, cyber security exercises |
| Secondary search terms (SST) | training, seminars, discussion exercises, serious games, exercise drill, function exercise, full-scaled exercise |
| Search string 1 (ST1) | ("information security management exercises" OR "cyber security management exercises" OR "management exercises in information security" OR "management exercises in cyber security" OR "information security exercises" OR "cyber security exercises") AND ("training" OR "seminars" OR "discussion exercises" OR "serious games" OR "exercise drill" OR "function exercises" OR "full-scaled exercises") |
| Search string 2 (ST2) | ("information security management exercises" OR "cyber security management exercises" OR "management exercises in information security" OR "management exercises in cyber security") AND ("training" OR "seminars" OR "discussion exercises" OR "serious games" OR "exercise drill" OR "function exercises" OR "full-scaled exercises") |

The findings from the search shows that expected results from a search only focusing on crisis management exercises would have missed relevant publications for the literature review (e.g., only 1 in the management search in Oria, whilst 7 when including information- and cyber security exercises). The number of search results are presented in table 13.

**Table 13. Results from search**

| Index/Database | Search | Total result |
|---|---|---|
| Scopus_1 | ST1 | 31 |
| Scopus_2 | ST2 | 1 |
| Oria_1 | ST1 | 97 |
| Oria-2 | ST2 | 1 |
| IEEE_1 | ST1 | 4 |
| IEEE_2 | ST2 | 0 |
| Springerlink_1 | ST1 | 0 |
| Springerlink_2 | ST2 | 0 |
| Science direct_1 | ST1 | 0 |
| Science direct_2 | ST2 | 0 |
| ACM_digital_library_1 | ST1 | 12 |
| ACM_digital_library_2 | ST2 | 0 |

In total n=14 relevant (by score) was found in the search. Only new results (not the same hit as in the first search) were added to the list from search _2. The n=14 relevant results are presented in the following sections.

A part of the literature review was to search for other literature reviews, and 3 literature reviews were found, but none of them focused on both information- and cyber security management and crisis management, and it appeared that there is not enough interdisciplinary research in the area.

Three lists were developed to cover the search, therein one annotated bibliography with in total 20 publications of interest for the scope of the research (6 score=2 was added to the original list). Upon analyzing the 20 publications, the numbers were narrowed down to only 13 publications being relevant. These publications are presented in the following sections 4.2.1) Relevant research from exercises in public organizations, 4.2.2) Relevant

research from exercises in other sectors, 4.2.3) Varieties of exercises, and 4.2.4) Learning activities.

### 4.2.1 Relevant research from exercises in public organizations

Dependent on nations ownership in critical infrastructures (e.g., electrical power plants in Norway), one publication was relevant for exercises in the public sector (Aoyama, B et al., 2017), in regard to "overlooking the importance of communication (e.g., the ability of a stakeholder to gather and provide relevant information)". A public-private partnership cybersecurity exercises in the Japanese government was found relevant (Watanabe, 2019) due to 1) "trust–based information sharing and coordinated incident responses", 2) "BIA (Business Impact Analysis) and SIA (Social Impact Analysis)", and 3) "interoperability among stakeholders". A relevant chapter about organizational issues relating to critical infrastructure information protection and thereby exercises in a book about cybersecurity culture (Trim & Upton, 2016) is also applicable for this research. The most relevant public exercises publication from the search was, however, Nicolova's experience-based publication about best practice for cybersecurity capacity building in Bulgaria's public sector (Nikolova, 2017). The publication also describes a developed framework for EXCON-work, a close match with the EXCON-publication written by Østby et. al (2019). Another publication presented a "free, open-source learning management system available online in conjunction with municipalities own security awareness materials to make a user-friendly training regiment that informed employees about potential threats" developed after a sophisticated spear-phishing campaign and thereby a cybersecurity survey of local government CIOs and CSOs in San Marcos, Texas (Prall, 2017). This is especially important in terms of how to develop scenarios based on previous events (Østby, Berg, et al., 2019). In addition, a publication presenting operative emergency-management support system tested in a cybersecurity exercise, testing ""Plan: What should we do?", "Do: What are we doing?", and "See: What kind of situations are we in?"" to support decision making in emergency management for cyber incidents (Kishi et al., 2017), was found relevant to redesign and use for future exercises.

### 4.2.2 Relevant research from exercises in other sectors

From other sectors an experienced based publication from a large national crisis management exercise for the financial sector in Sweden in 2021 (Varga et al., 2021), where the learning outcomes showed "information about rational adversaries that cause prolonged disturbances is possibly not collected, analyzed, and utilized systematically. Much effort was put into ensuring that timely and relevant information from organizations is shared in an efficient manner." (Varga et al., 2021) The "relevant information shared in efficient manner" is especially relevant in the studies considering escalation and de-escalation of information in my research (Østby et al., 2020; Østby & Katt, 2019a; Østby & Kowalski, 2021, 2022c). From the search it was also found a crisis management system called KADAN which was developed for crisis response during the 2017 Sapporo Asian Winter Games (Kosaka et al., 2019), and as mentioned in the findings, "even though it is not accurately relevant for information- and cybersecurity incidents, it gives a good example of how crisis management can be combined with already planned governance and operation process, presenting a type of both a standard Crisis Information Management system (CIM) and Security Information Management and Event Management (SIEM)-report relevant in a crisis".

### 4.2.3 Variety of exercises from the literature search

Gurnani et al. suggest a planning for exercise framework where cybersecurity exercises can be divided into two groups, one group for seminars, workshops, discussion exercises, table-tops and games in the framework of discussions, and one group for drills, functional and full-scaled exercises in the framework of operation-based exercises (Gurnani et al., 2014). We also found this separation (discussion vs. operation-based) in a publication which had made a game-exercise tool based on learning goals (Omiya & Kadobayashi, 2019). Timely, we have arranged full-scaled exercises allowing discussions and learning goals for collaborations based on the guidance from Homeland Security Exercise and Evaluation Program (HSEEP), suggesting that a full-scale exercise should have the content of both (HSEEP, 2006). Also, Trim & Upton have in their book limited their scope of exercises to table-top exercises and simulation exercises (Trim & Upton, 2016) which may be suggested limited to the possibilities to provide targeted exercises for different students, groups, and organizations. However, the mentioned suggested framework presented in Nikolova (2017) with necessary redesign to a variety of exercises (not only full-scaled exercises) is better suited and more in line with the experiences we have from the Norwegian Cyber Range to meet the mentioned needs.

### 4.2.4 Learning activities

Grimaila (2004) has over "a three-year period developed and implemented a scenario-based, information security management exercise" in an information security course at Texas A&M University. The learning activities like "hands on experience in the planning, analysis, design, implementation, and maintenance of an organization's information security program" in that course is relevant to the ongoing triple-loop-learning activities in the IMT-4115 Introduction to information security management course at NTNU (Østby & Kowalski, 2022b). In addition, White presents "the use of scenario-based exercises in addressing security issues common to large organizations, industry sectors, and various levels of government." (White et al., 2004), also relevant to the work on preparing scenarios for exercises (Østby, Berg, et al., 2019). Another important issue on how to prepare for learning activities is that "measuring learning using the NIST NICE framework has shown that cybersecurity exercises will improve cybersecurity knowledge" (Karjalainen et al., 2020).

## 4.3 Summary

The literature review indicates that redesign of existing exercises in similar organizations, learning activities from relevant studies, and existing guidelines is necessary. Adapting learning artifacts from existing literature about information security crisis management in public emergency organizations, have provided necessary development throughout the study. The rigorous literature review also provided us with results from other organizations, a variety of exercises, and especially learning activities from these exercises. The thematic overview of our analysis in this chapter is presented in figure 26.

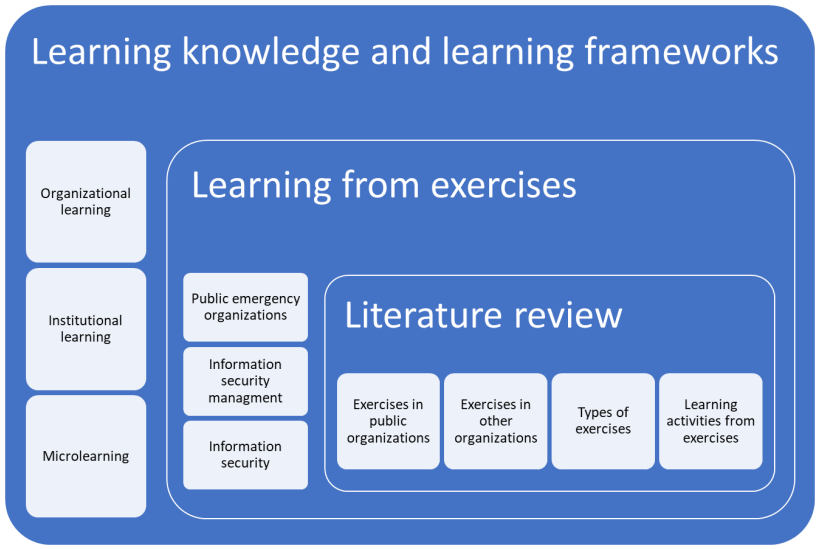



**Fig. 26.** Thematic rigor and relevance analysis

Analyzing the results thematically as presented in figure 26, we were able to establish from literature what has been done before and discuss the relevance to adapt and modify our framework.

# 5 Concluding remarks and ongoing and future research directions

The research has taken place as a part of the Norwegian Cyber Range innovation project (NTNU, 2019c), and the research contribution has focused top-down from the society level through the digital value chain level and touched on the digital cyber infrastructure level of the project. For the full-scaled exercises however, a collaboration between the different areas of interests at the NCR has been necessary. The contribution from this research can be presented as presented with red in figure 27.

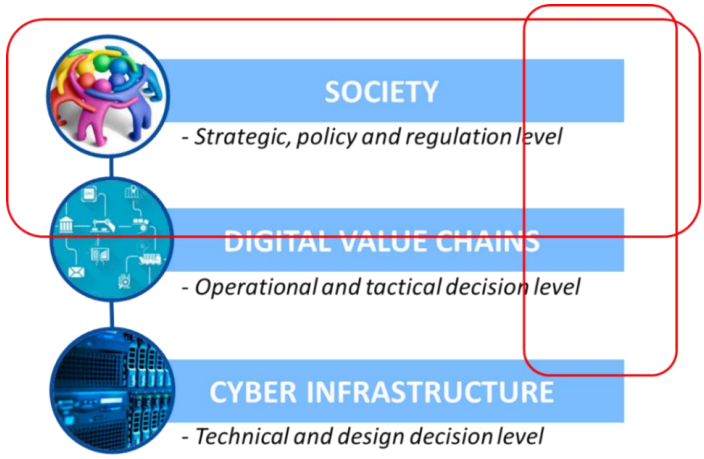



**Fig. 27.** Contribution in the Norwegian Cyber Range project framework

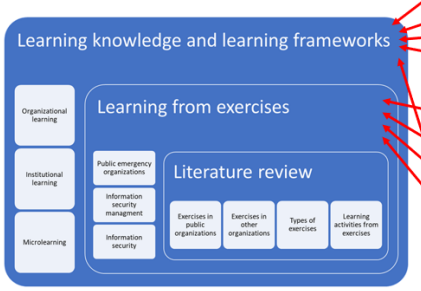
The work in this research project have tried to mitigate the resilience and readiness gap with awareness from case-studies, suggested learning artifacts for organizations, institutions, and individuals through preparations for and execution of exercises. Morover, how this knowledge can be implemented in training and exercises at the Norwegian Cyber Range and in other cyber-ranges. The thesis summary also presents a novel holistic socio-technical approach to prepare for organizational exercises to respond to cyber-attacks, and also user-centric approaches to build robust EXCON-teams for the exercises.

Results from the exercises and learning artifacts presents a change in knowledge, skills and competence. Whether this is adaptive or transformative change can be related to the maturity and readiness in the organizations or amongst the students.

Furthermore this thesis summary presents ongoing attempts to train students in incident response through management learning artifacts necessary in information- and cybersecurity crisis management situations. Results from triple-loop-learning evaluation shows that the students are able to evaluate their own learning outcome and are able to adapt the learning-artifacts presented to them.

Along with the thematic overview (figure 26) of the analysis **existing knowledge**, a mapping of this project's **publications** and the analysis of **case-studies and exercises** presented in section 3 in this thesis summary. It was found that the preparation for

exercises framework and how to build EXCON teams for full-scaled information- and cyber security exercises has received little attention in the research community, and also in regard to societal training for readiness and resilience when experiencing a cyber-attack. The mapping is presented in figure 28 and the two publications are marked with red.




| | |
|---|---|
| Publication 1 | Østby, Grethe; Kowalski, Stewart James. (2021) A case study of a municipality phishing attack measures - towards a socio-technical incident management framework. *CEUR Workshop Proceedings. vol. 3016.* |
| Publication 2 | Østby, Grethe; Kowalski, Stewart James; Katt, Basel. (2020) Towards a Maturity Improvement Process – Systemically Closing the Socio-Technical Gap. *CEUR Workshop Proceedings. vol. 2789.* |
| Publication 3 | Østby, Grethe; Kowalski, Stewart James. (2022) ORGANIZATIONAL LEARNING WITH CRISES. *EDULEARN22 Proceedings.* lated. |
| Publication 4 | Østby, Grethe; Katt, Basel. (2019) Cyber Crisis Management Roles – A Municipality Responsibility Case Study. *Information Technology in Disaster Risk Reduction.* Springer. |
| Publication 5 | Østby, Grethe; Kowalski, Stewart James. (2022) Introducing Serious Games as a Master Course in Information Security Management Programs: Moving Towards Socio-Technical Incident Response Learning. *Handbook of Research on Cross-Disciplinary Uses of Gamification in Organizations.* IGI Publishing. |
| Publication 6 | Østby, Grethe; Kowalski, Stewart James. (2020) Preparing for cyber crisis management exercises. *Augmented Cognition. Human Cognition and Behavior.* Springer. |
| Publication 7 | Østby, Grethe; Lovell, Kieren N.; Katt, Basel. (2020) EXCON Teams in Cyber Security Training. *2019 International Conference on Computational Science and Computational Intelligence (CSCI).* IEEE. |
| Publication 8 | Østby, Grethe; Berg, Lars; Kianpour, Mazaher; Katt, Basel; Kowalski, Stewart James. (2019) A Socio-Technical Framework to Improve cyber security training: A Work in Progress. *CEUR Workshop Proceedings. vol. 2398.* |
| Appendix 1 | Hendelseshåndtering ved cyber-angrepet mot Østre Toten kommune https://www.ototen.no/aktuelt/rapport-etter-dataangrepet.15279.aspx |

**Fig. 28.** Conclusions from thematic mapping of publications

Publication 3 and publication 5 presents frameworks to learn information security management through discussion exercises and through creating games in management courses. These are similar to other ongoing student-activities (see section 4.2), but the content of using 1) triple-loop-learning in publication 3, and 2) scoping development of serious games for information- and cyber security incident response in publication 5, are not found in the literature search.

In addition, these 4 publications (6, 7, 3, and 5), the 'train-the-trainer' concept from Selebø's master thesis (Selebø, 2022) has been accepted to be presented at the AHFE conference in San Francisco 2023 (Østby et al., 2022). There, we will present results from the in-depth interviews which were conducted with information security and/or exercise experts from different Norwegian organizations with relevant EXCON experience, together with results from EXCON-evaluations from exercises executed at the Norwegian Cyber Range.

Presenting results from exercise Morris (NTNU, 2022) including mapping of information sharing are a work in progress, where information sharing and information sharing platforms regarding crisis management during cyber-attacks are of special interest.

The analysis of the **learning activities** presented in section 3 and in the **literature review**, concludes with fine-tuned coordinated learning activities to meet the timeline of a scenario (figure 23), and triple-loop-learning activities for use in the timeline in figure 21. The user-centric-approach in figure 15 is however of importance to be able to

implement the activities at the right level in the organization and to close the gap one step at the time (figure 25). This process is presented in figure 29.

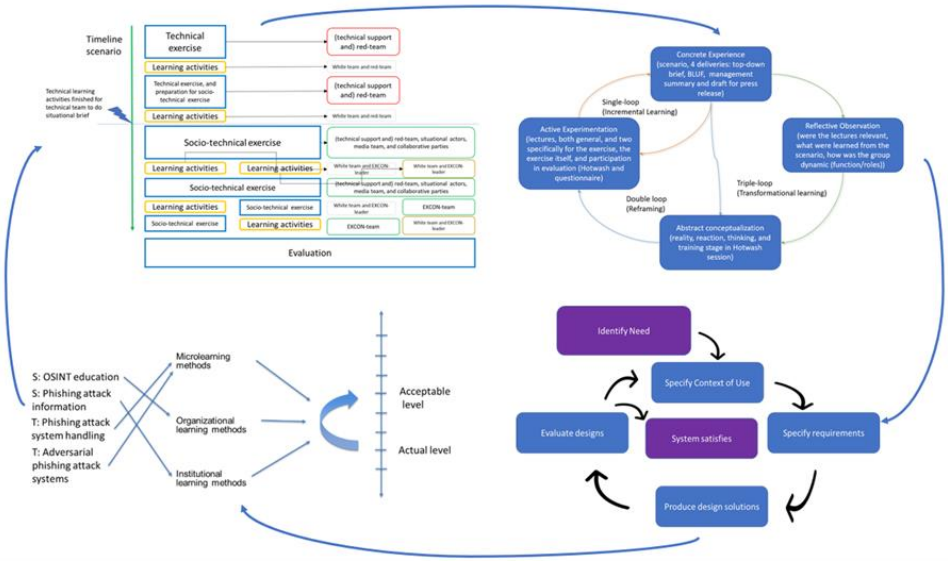



**Fig. 29.** Coordinated learning activities

Socio-technical learning activities are presented in publication 1, 2, 3 and 8, and the analysis in section 3 concludes that 1) targeted exercise goals developed in the scenarios are met during the exercises, 2) socio-technical step-by-step improvement can be developed based on the level of escalation maturity, and 3) organizations can learn from training and exercises.

It is necessary to further investigate socio-technical learning artifacts in exercises for years to come. The need to develop such learning artifacts should also be developed with societal changes in the digital environment accordingly and in line with change management responsibilities and ongoing need for training and exercises.

Finally, the analysis from appendix 1(partly translated and presented in section 3.1) concludes how important and what roles based on publication 4 should be covered in a municipality emergency plan, and in other organizations as well.

# 6 Epilog (see English below)

Under midtveisevalueringen reflekterte jeg over å være midtveis i livet samtidig som jeg var midtveis i PhD-løpet, og skjelnet til et dikt av Inger Hagerup kalt «Å disse fiolette morgentimer»:

Å, disse fiolette morgentimer
når tiden ennå er en våken drøm
og gleden går i store, blanke stimer
igjennom sinnets klare understrøm.

Når jord og himmel er en gjennomsiktig
bekreftelse på dét at du er til,
og alt er godt og ingenting er viktig
unntagen noe skinnende du vil

med dette ufødte som hviler i deg
og rolig lengter etter å bli brukt,
som fugleungens vinger bærer i seg
sin sommerhimmel og sin himmelflukt.

Fra diktsamlingen «Strofe med vinden», Aschehoug 1958

Jeg har nå forsøkt å formidle hva jeg har funnet, hva jeg har lært, og ikke minst hva som gjenstår av arbeid. Mitt PhD-arbeid er ved veis ende, men det er absolutt ikke forskningen på området. Søken etter kunnskap og ferdigheter har alltid vært en stor del av meg, og aldri har jeg fryktet å feile intellektuelt da det ofte gir den beste læringen for å omsette læringen til mer korrekte ferdigheter – da uten at det går ut over andre. Jeg har alltid trivdes ved skolebenken, men nå er den tiden over. «Jeg fant, jeg fant» sa Askeladden, og det har jeg jammen gjort. Selv om prinsen og halve kongeriket har latt vente på seg, har jeg hatt mange gode hjelpere og fått mange nye spennende bekjentskaper som jeg har kunnet rådføre meg med. Med takknemlighet i hjertet vil jeg derfor avslutte denne ferden med et dikt fra Bente Bratlund (Mærland), "Å dryssa stjerner", 1991.

Vi treng håpet.
Den vesle kvite perla ein stad i oss,
gøymt. Den stille elva som brått kan
brusa over. Utsynet bak neste sving.
Tonen som løftar dagen.
Vi treng handa som løftar fram
og orda som vekkjer draumar.
Løvetannen opp or asfalten.
Fuglen på veg i fridomen,
lyset på skrå inn.
Håpet vi kan gje kvarandre,
eller ta bort.
Denne dagen er vår.

# 7 Epilogue English

During the mid-term evaluation, I reflected on being in the middle of life at the same time as I was in the middle of the PhD course, and discerned a poem by Inger Hagerup called "Oh these violet morning hours":

Poem by Inger Hagerup
Oh, these violet morning hours

Oh, those violet morning hours
when time is still a waking dream
and the joy goes in large, shiny shoals
through the clear undercurrent of the mind.

When earth and sky are transparent
confirmation that you exist,
and everything is good, and nothing is important
except something shiny you want to do

with this unborn that rests in you
and calmly longs to be used,
which the baby bird's wings carry
his summer sky and his escape to heaven.

From the collection of poems «Strophe with the wind» Aschehoug, 1958

I have now tried to convey what I have found, what I have learned, and not least what remains. My PhD work is completed, but the research in the area is certainly not. The search for knowledge and skills has always been in my ways, and I have never feared to fail intellectually as it often provides the best learning to get the proper skills - then without it affecting others. I have always thrived at school, but now that time is over. "I found, I found," said Askeladden, and I certainly have. Even though the prince and half the kingdom are still waiting, I have had the pleasure of meeting many good helpers and made many exciting new acquaintances throughout these years. With gratitude in my heart, I will therefore end this journey with a poem from Bente Bratlund (Mærland), "To spread stars", 1991.

We need hope.
The tiny white pearl has a place in us,
hidden. The quiet river that suddenly can
shower over. The view behind the next bend.
The tone that lifts the day.
We need the hand that lifts us forward
and the words that awaken dreams.
The dandelion up on the asphalt.
The bird on its way to freedom,
the light at an angle.
The hope we can give each other,
or take away.
This day is ours.

# 8 References


Ackerman, M. S. (2000). Intellectual challenge of CSCW: the gap between social requirements and technical feasibility. *Human-Computer Interaction*, *15*(2–3), 179–203. https://doi.org/10.1207/S15327051HCI1523_5

Anderson, E. (2017). *HOW TO COMPLY WITH THE 5 FUNCTIONS OF THE NIST CYBERSECURITY FRAMEWORK*. FORESCOUT. https://www.secmatters.com/blog/how-to-comply-with-the-5-functions-of-the-nist-cybersecurity-framework

Aoyama, B, T., Watanabe, K., & Koshijima, I. (2017). Developing a Cyber Incident Communication Management Exercise for CI Stakeholders. *Critical Information Infrastructures Security. CRITIS 2016.*, *November*. https://doi.org/10.1007/978-3-319-71368-7

Atlantic_Council. (2021). *Cyber 9/12 Strategy Challenge*. https://www.gcsp.ch/events/cyber-912-strategy-challenge-2021

Bass, B. M. (2000). The Future of Leadership in Learning Organizations. *The Journal of Leadership Studies*, *7*(3), 18–40. https://journals.sagepub.com/doi/pdf/10.1177/107179190000700302?casa_token=I38n1NBuDzAAAAAA:zYRRSK7AAP3ijro4tUgksVi1eyMZ9laHZm8ZT1BLPUuxMnqBqF126vZ_apPjXnVhtGdit2Q_tyiaQA

Boin, A., & Hart, P. (2001). *Public Leadership in Times of Crisis : Mission Impossible ? Crisis : A Window for Leadership ? Consciousness : Leadership Challenges*.

Chalmers, A. (1999). What Is This Thing Called Science. In *Hackett Publishing Company* (3rd ed.). Hackett Publishing. https://mycourses.aalto.fi/pluginfile.php/1139027/mod_resource/content/1/WhatIsThisThingCalledScience-Chalmers-1999.pdf

Cisco. (2018). *Annual cyber security report*.

Comfort, L. K. (2007). Crisis management in hindsight: Cognition, communication, coordination, and control. *Public Administration Review*, *67*(SUPPL. 1), 189–197. https://doi.org/10.1111/j.1540-6210.2007.00827.x

ctftech.com. (2022, October). *Cybercation - Nordic-Baltic educators' forum*. Ctftech.Com.

Veileder i planlegging, gjennomføring og evaluering av øvelser - grunnbok, (2016). https://www.dsb.no/veiledere-handboker-og-informasjonsmateriell/grunnbok-oving/

DSB. (2018). *Veileder til forskrift om kommunal beredskapsplikt*. DSB. https://www.dsb.no/veiledere-handboker-og-informasjonsmateriell/veileder-til-forskrift-om-kommunal-beredskapsplikt/

DSB. (2019). *DISASTERS THAT MAY AFFECT NORWEGIAN SOCIETY*. https://www.dsb.no/globalassets/dokumenter/rapporter/p2001636_aks_2019_eng.pdf

DSB. (2020). *Øvelse digital 2020*. Dsb.No.

Dumitru, S. (2016). the Cyber Dimension of Modern Hybrid Warfare and Its Relevance for Nato. *Europolity: Continuity and Change in European Governance*, *10*(1), 7–23.

ENISA. (2009). *Good Practice Guide on National Exercises Enhancing the Resilience of Public Communications Networks Good Practice Guide on Exercises 2 Good Practice Guide on National Exercises*. http://www.enisa.europa.eu/act/res

Entertainment software association. (2022, January 18). U.S. Consumer Video Game Spending Totaled $60.4 Billion in 2021. *CICION Pr Netwire*.

European Parliament. (2017). *Digital Economy and Society Index (DESI)*. file:///C:/Users/grethos/Downloads/no_desi_country_profile_43206.pdf
Geels, F. G. (2005). *Technological Transitions and System Innovations: A Co-evolutionary and Socio-technical Analysis*. Edvard Elgar publishing limited.
Grimaila, M. R. (2004). A novel scenario-based information security management exercise. *2004 Information Security Curriculum Development Conference, InfoSecCD 2004*, 66–70. https://doi.org/10.1145/1059524.1059538
Gurnani, R., Pandey, K., & Rai, S. K. (2014). A scalable model for implementing cyber security exercises. *2014 International Conference on Computing for Sustainable Global Development, INDIACom 2014*, 680–684. https://doi.org/10.1109/IndiaCom.2014.6828048
Haimes, Y. Y. (2009). On the complex definition of risk: A systems-based approach. In *Risk Analysis*. https://doi.org/10.1111/j.1539-6924.2009.01310.x
Hainey, T., Connolly, T., Stansfield, M., & Boyle, L. (2011). The Use of Computer Games in Education: A Review of the Literature. In *Handbook of Research on Improving Learning and Motivation through Educational Games: Multidisciplinary Approaches* (pp. 29–50). IGI Publishing.
Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Two Paradigms on Research Essay Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–79. https://www.jstor.org/stable/25148625?seq=1#metadata_info_tab_contents
Horni, K. (2020). Grethe fra Lena skal ta doktorgrad på cyber-sikkerhet. *Totens Blad*.
HSEEP. (2006). *Homeland Security Exercise and Evaluation Program Volume 1: HSEEP Overview and Exercise Program Management*. http://hseep.dhs.gov.
Huseby, J. O. V. (2021). *SIEMS-CIMS integration: Secure upload of cyber-incident information to crisis information management systems* [Master-thesis]. NTNU.
immuta.com. (2021). *Data redaction*. Immuta.Com. https://www.immuta.com/blog/what-is-data-redaction/
Jørgenrud, M. (2017, May 9). Overtar IT-drift i fem Østfold-kommuner: – Avtalen er verdt en halv milliard. *Digi.No*.
Justis- og beredskapsdepartementet. (2010). *Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (sivilbeskyttelsesloven)*. Norwegian Government. https://lovdata.no/dokument/NL/lov/2010-06-25-45?q=lov om kommunal beredskapsplikt
Karokola, G., Kowalski, S., & Yngström, L. (2011). Secure e-government services: Towards a framework for integrating IT security services into e-government maturity models. *2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference*. https://doi.org/10.1109/ISSA.2011.6027525
Karokola, G. R. (2012). *A framework for Securing a-Government Services, The case of Tanzania*. Stockholm University.
Kemmis, S., McTaggart, R., & Nixon, R. (2014). *The Action Research Planner*. Springer Science+Business Media Singapore. https://doi.org/10.1007/978-981-4560-67-2
Kishi, K., Kosaka, N., Kura, T., Kokogawa, T., & Maeda, Y. (2017). Study on Integrated Risk-Management Support System. *ISCRAM 2017 Conference*, *May 2017*, 432–444.
Koingharara, S. S. (2022, February 28). *DEDUCTION, INDUCTION AND ABDUCTION IN ACADEMIC WRITING*. Seansturm.Wordpress.Com.
Kosaka, N., Koyama, A., Kura, T., Kishi, K., Kokogawa, T., & Maeda, Y. (2019). Applicability Assessment of an Emergency Management Support System "KADAN." *2019 IEEE International Conference on Big Data and Smart Computing, BigComp 2019 - Proceedings*. https://doi.org/10.1109/BIGCOMP.2019.8679466

Koutromanos, G., Sofos, A., & Avraamidou, L. (2015). The use of augmented reality games in education: a review of the literature. *Educational Media International*, *52*(4), 253–271. https://doi.org/10.1080/09523987.2015.1125988

Kowalski, S. (1994). *IT Insecurity: A Multi-disiplinary Inquiry*. Stockholm University.

Kuechler, W., & Vaishnavi, V. (2012). A Framework for Theory Development in Design Science Research: Multiple Perspectives. In *Journal of the Association for Information Systems* (Vol. 13, Issue 6).

Kvie Lundevall, E. (2020). Hvordan kan du forberede organisasjonen din på et dataangrep? *Sikkerhet, NSO*, 39–41.

Lagadec, P. (1997). *Learning Processes for Crisis Management in Complex Organizations*. *5*(1), 24–31.

Lalonde, C., & Roux-dufort, C. (2013). *Challenges in Teaching Crisis Management : Connecting Theories , Skills , and Reflexivity*. https://doi.org/10.1177/1052562912456144

Leavitt, H. (1965). Applying Organizational Change in Industry: Structural, Technological, and Humanistic Approaches. In J. G. March (Ed.), *Handbook of organizations* (pp. 1144–1170). https://scholar.google.com/scholar?as_q=Applied+organizational+change+in+industry%3A+Structural%2C+technological+and+humanistic+approaches&as_occt=title&hl=en&as_sdt=0%2C31

Lunde, I. K. (2019). *Praktisk krise- og beredskapsledelse. etablering av beredskap - potensialbasert beredskapsledelse - proaktiv stabsmetodikk* (2nd ed.). Universitetsforlaget. https://www.ark.no/boker/Ivar-Konrad-Lunde-Praktisk-krise-og-beredskapsledelse-9788215031866?gclsrc=aw.ds&gclid=Cj0KCQiA-eeMBhCpARIsAAZfxZBn_e1322BDk4ZUIRerex3e7ARhoeq9Y8lRGmjAk8caBI_8MEbuk18aAodaEALw_wcB#product-description

Marion, R., & Uhl-Bien, M. (2001). Leadership in complex organizations. *The Leadership Quarterly*, *12*(2001), 381–418. file:///C:/Users/grethos/Downloads/1-s2.0-S1048984301000923-main.pdf

Mathisen, G. (2021). Øver seg frem til doktorgrad. *Aktuell Sikkerhet*, 36–37.

Medema, W., Wals, A. E. J., & Adamowski, J. F. (2014). *Multi-Loop Social Learning for Sustainable Land and Water Governance : Towards a Research Agenda on the Potential of Virtual Learning Platforms*. *July 2018*. https://doi.org/10.1016/j.njas.2014.03.003

Mostafa, M., & Faragallah, O. S. (2019). Development of Serious Games for Teaching Information Security Courses. *IEEE Access*, *7*, 169293–169305. https://doi.org/10.1109/ACCESS.2019.2955639

Mumford, E. (2006). The story of socio-technical design: Reflections on its successes, failures and potential. In *Information Systems Journal*. https://doi.org/10.1111/j.1365-2575.2006.00221.x

Muntean, C. I. (2011). Raising engagement in e-learning through gamification. *The 6th International Conference on Virtual Learning ICVL 2011*. http://en.wikipedia.org/wiki/Gamification

Nasjonal Sikkerhetsmyndighet. (2017). *Rammeverk for håndtering av IKT-sikkerhetshendelser*. 1–20. https://www.nsm.stat.no/globalassets/dokumenter/vedlegg-til-rammeverk-for-handtering-av-ikt-hendelser/rammeverk-for-handtering-av-ikt-sikkerhetshendelser.pdf

Nemeth, C., Wears, R. L., Patel, S., Rosen, G., & Cook, R. (2011). Resilience is not control: Healthcare, crisis management, and ICT. *Cognition, Technology and Work*. https://doi.org/10.1007/s10111-011-0174-7

Nikolova, I. (2017). Best Practice for Cybersecurity Capacity Building in Bulgaria's Public Sector. *Information & Security: An International Journal*, *38*, 79–92. https://doi.org/10.11610/isij.3806

Norwegian Data inspectorate. (2018). *Trust and emotions*.

NSM, DSB, Digitaliseringsdirektoratet, NTNU, & NorSIS. (2020). *ovelse.no*. https://ovelse.no/

NTNU. (2019a). *GUIDE FOR DESIGN OF STUDY PROGRAMMES AND COURSES AT NTNU ( THE PROGRAMME DESCRIPTION GUIDE )*.

NTNU. (2019b). *REQUIREMENTS FOR THE ACADEMIC PORTFOLIO AT NTNU*.

NTNU. (2019c). *The Norwegian Cyber Range*. https://www.ntnu.no/ncr

NTNU. (2021). *IMT4115 - Introduction to Information Security Management*. https://www.ntnu.edu/studies/courses/IMT4115/2021/1#tab=omEmnet

NTNU. (2022, September 29). *Øvelse Morris*. https://www.ntnu.no/ncr/morris

Nyheim, M. (2022, October 13). Sykehus benyttet NTNUs øvingsarena for øvelse i cybersikkerhet. *NTNU Nyheter*.

Omiya, T., & Kadobayashi, Y. (2019). Secu-One: A proposal of cyber security exercise tool for improving security management skill. *PervasiveHealth: Pervasive Computing Technologies for Healthcare*, *Part F1483*, 259–268. https://doi.org/10.1145/3323771.3323792

Østby, G. ;, Berg, L. ;, Kianpour, M. ;, Katt, B. ;, & Kowalski, S. (2019). *A Socio-Technical Framework to Improve cyber security training: A Work in Progress*. https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2624957

Østby, G., & Katt, B. (2019a). Cyber Crisis Management Roles – A Municipality Responsibility Case Study. In *Science and Technology in Disaster Risk Reduction in Asia* (pp. 168–181). https://doi.org/10.1016/b978-0-12-812711-7.00014-6

Østby, G., & Katt, B. (2019b). *Maturity modelling to prepare for cyber crisis escalation and management*.

Østby, G., & Kowalski, S. J. (2020). Preparing for Cyber Crisis Management Exercises. *N: Schmorrow D., Fidopiastis C. (Eds) Augmented Cognition. Human Cognition and Behavior. HCII 2020. Lecture Notes in Computer Science, Vol 12197.*, 279–290. https://doi.org/https://doi.org/10.1007/978-3-030-50439-7_19

Østby, G., & Kowalski, S. J. (2021). A case study of a municipality phishing attack measures - towards a socio-technical incident management framework. *CEUR*. https://drive.google.com/file/d/1ekj9YKAYUdGpIeB9L8zxKvffSUDnFn9L/view

Østby, G., & Kowalski, S. J. (2022a). Introducing Serious Games as a Master Course in Information Security Management Programs: Moving Towards Socio-Technical Incident Response Learning. In O. Bernades, V. Amorim, & A. Moreira (Eds.), *Handbook of Research on Cross-Disciplinary Uses of Gamification in Organizations* (p. 24). IGI Global. https://doi.org/10.4018/978-1-7998-9223-6.ch023

Østby, G., & Kowalski, S. J. (2022b). ORGANIZATIONAL LEARNING WITH CRISES-TRIPLE LOOP LEARNING IN CYBER SECURITY EXERCISES. *EDULEARN22*, 5215–5224. https://library.iated.org/?search_text=publication%3AEDULEARN22&adv_title=&rpp=25&adv_authors=%C3%98stby&adv_keywords=&orderby=page&fulltext=on&refined_text=

Østby, G., & Kowalski, S. J. (2022c). *Hendelseshåndtering ved cyberangrepet mot Østre Toten kommune*.

Østby, G., Kowalski, S. J., & Katt, B. (2020). Towards a Maturity Improvement Process – Systemically Closing the Socio-Technical Gap. *6th International Workshop on Socio-Technical Perspective in IS Development - STPIS*, 195–205. http://ceur-ws.org/Vol-2789/paper26.pdf

Østby, G., Lovell, K. N., & Katt, B. (2019). EXCON teams in cyber security training. *Proceedings - 6th Annual Conference on Computational Science and Computational Intelligence, CSCI 2019*, 14–19. https://doi.org/10.1109/CSCI49370.2019.00010

Østby, G., Selebø, B. E., & Kowalski, S. (2022). Training the Trainers for Cybersecurity Exercises - Developing EXCON-teams. *AHFE 2023*. https://www.ahfe-cms.org/author#/ViewPaper/862

Pahl-Wostl, C., Becker, G., Knieper, C., & Sendzimir, J. (2013). How multilevel societal learning processes facilitate transformative change: A comparative case study analysis on flood management. *Ecology and Society*, *18*(4). https://doi.org/10.5751/ES-05779-180458

Parmigiani, G., & Inoue, L. (2009). *Decision Theory: Principles and Approaches* (D. J. BALDING, N. A. C. CRESSIE, G. M. FITZMAURICE, I. M. JOHNSTONE, G. MOLENBERGHS, D. W. SCOTT, A. F. M. SMITH, R. S. TSAY, S. WEISBERG, & H. GOLDSTEIN, Eds.). John Wiley & Sons. https://www.webdepot.umontreal.ca/Usagers/perronf/MonDepotPublic/stt2100/Decision_theory.pdf

Prall, D. (2017). The weakest link in your cybersecurity chain. *American City and County*, *132*(5), 14–18.

Riksrevisjonen. (2019). *Undersøkelse av angrep mot IKT-systemer i politiet*. https://www.riksrevisjonen.no/rapporter-mappe/no-2019-2020/undersokelse-av-angrep-mot-ikt-systemer-i-politiet/

Riksrevisjonen. (2020). *Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer*. https://www.riksrevisjonen.no/rapporter-mappe/no-2020-2021/undersokelse-av-helseforetakenes-forebygging-av-angrep-mot-sine-ikt-systemer/

Rooney, J. J., & vanden Heuvel, L. N. (2004). *Root Cause Analysis For Beginners*. www.asq.org

Saavedra, V., Dávila, A., Melendez, K., & Pessoa, M. (2017). Organizational Maturity Models Architectures: A Systematic Literature Review. In *Advances in Intelligent Systems and Computing* (Vol. 537). https://doi.org/10.1007/978-3-319-48523-2_3

Saunders, M., Lewis, P., & Thornhill, A. (2012). *Research Methods for Business Students* (6th ed.). https://gibsoncollege.edu.et/wp-content/uploads/2022/01/Research-Methods-for-Business-Students-by-Mark-Saunders-Philip-Lewis-Adrian-Thornhill-z-lib.org-1.pdf

Scarfone, K., Grance, T., & Masone, K. (2008). *Computer Security Incident Handling Guide*. https://csrc.nist.rip/library/NIST%20SP%20800-061r1%20Computer%20Security%20Incident%20Handling%20Guide,%202008-05.pdf

Selebø, B. E. (2022). *Preparing for cyber-incident exercises: Developing best practice within exercise control management (EXCON)* [Master thesis, NTNU]. https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3007605

Sikkerhetsfestivalen. (2019). *Megagame*. https://sikkerhetsfestivalen.no/bidrag2019/megagame

Staveli, M. B. (2020). Gjøvik stopper e-poster med vedlegg etter hackingskandalen. *Oa.No*. https://www.oa.no/gjovik-stopper-e-poster-med-vedlegg-etter-hackingskandalen/s/5-35-1157368

Capability Maturity Model® Integration (CMMISM), (2002). ftp://ftp.sei.cmu.edu/public/documents/02.reports/pdf/02tr028.pdf

The Norwegian Business and Industry Security Council. (2020). *The dark numbers survey 2020*. https://www.nsr-org.no/aktuelt/mørketallsundersøkelsen-2020

The Norwegian Government. (2019a). *Nasjonal strategi for digital sikkerhet | 1 Nasjonal strategi for digital sikkerhet Departementene*. https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf

The Norwegian Government. (2019b). *Tiltaksoversikt til nasjonal strategi for digital sikkerhet | 1 Tiltaksoversikt til nasjonal strategi for digital sikkerhet Departementene*. https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/tiltaksoversikt---nasjonal-strategi-for-digital-sikkerhet.pdf

One digital public sector, regjeringen.no (2019).

The Norwegian Justice- and emergency department. (2015). Instruks for statsforvalteren og Sysselmesteren på Svalbard sitt arbeid med samfunnssikkerhet, beredskap og krisehåndtering. In *Lovdata*.

The Norwegian justice and police department. (2000). *Et sårbart samfunn*. Et sårbart samfunn

Trim, P., & Upton, D. (2016). *Cyber security culture*. Routledge. https://web.p.ebscohost.com/ehost/ebookviewer/ebook/bmxlYmtfXzUwNDY0Ml9fQU41?sid=06d50025-30bf-47f4-80ba-059b979a8261@redis&vid=0&format=EB&rid=1

User-centered design (UCD) process, (2021). https://www.usability.gov/what-and-why/user-centered-design.html#:~:text=User-Centered Design Process&text=Design is based upon an,process and it is iterative.

Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk. *Computers & Security*, *105*, 102239. https://doi.org/10.1016/j.cose.2021.102239

Velazquez, L. E., Esquer, J., Munguía, N. E., & Moure-Eraso, R. (2011). Sustainable learning organizations. *Learning Organization*, *18*(1), 36–44. https://doi.org/10.1108/09696471111095984

Wahlgren, G., & Kowalski, S. (2016). A Maturity Model for Measuring Organizations Escalation Capability of IT-related Security Incidents in Sweden. *Assosiation for Information Systems*.

Watanabe, K. (2019). PPP (public-private partnership)-based cyber resilience enhancement efforts for national critical infrastructures protection in Japan. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 11260 LNCS*. Springer International Publishing. https://doi.org/10.1007/978-3-030-05849-4_13

Watts, J., Mackay, R., Horton, D., Hall, A., Douthwaite, B., Chambers, R., & Acosta, A. (2007). *ILAC Working Paper 3 Institutional Learning and Change: An Introduction*. www.cgiar-ilac.org

Whitman, M. E., & Mattord, H. J. (2018). *Management of Information Security*. Cengage. https://www.adlibris.com/no/bok/management-of-information-security-9781337405713?gclid=CjwKCAjwo4mIBhBsEiwAKgzXONCA2b5KlFWEPgb7kC7L6GGT8O-nUzmz0Y3Mx4YJ0IinwIxJrGs6WRoCE5QQAvD_BwE

Xie, L. (2019). Leadership and organizational learning culture: a systematic literature review. In *European Journal of Training and Development* (Vol. 43, Issues 1–2, pp. 76–104). Emerald Group Holdings Ltd. https://doi.org/10.1108/EJTD-06-2018-0056

Yale. (2019). *Intendent learning outcomes*. https://poorvucenter.yale.edu/IntendedLearningOutcomes

Zegzhda, D. P. (2016). Sustainability as a criterion for information security in cyber-physical systems. *Automatic Control and Computer Sciences*, *50*(8), 813–819. https://doi.org/10.3103/S0146411616080253

# 9 Publications

Publication 1

Østby, Grethe; Kowalski, Stewart James. (2021) A case study of a municipality phishing attack measures - towards a socio-technical incident management framework. *CEUR Workshop Proceedings. vol. 3016.*

# A case study of a municipality phishing attack measures - towards a socio-technical incident management framework

Grethe Østby [1], Stewart James Kowalski [1]

[1] *Norwegian University of Science and Technology, Teknologiveien 22, Gjøvik, Innlandet, Norway*

**Abstract**

During the Corona-crisis, the number of data breaches and hacking increased rapidly. For some organizations it was difficult to handle both the Corona-crises and such attacks. A decision made to prevent this overload of crisis, happened in Gjøvik municipality, where they closed their email-system and shut down macros in their applications to prevent an overload situation. In this work-in-progress paper, we have analyzed their decision in a combined socio-technical and crisis management context and suggest such framework to do analysis and make right decisions to prevent data breaches and other organizational cyber-crimes from succeeding, but also to prevent an overload of crisis situations at the same time.

**Keywords** [1]

Incident management, Data breaches prevention, Cyber-attack prevention, Socio-technical analysis, Crisis management analyses, SBC-analyses, NIST-analyses.

## 1. Introduction

Recent studies in Norway show that cyber-attacks on organizations are increasing both in quantity and in scope [1]. The results also suggest a clear shift from attack on machines to attack on humans.

The Norwegian Parliament was subject to such a social engineering attack in August 2020 [2], [3]. A spear phishing attack against several email-accounts took place. In the Parliament several technical measures had been previously implemented, but new social engineering attack approaches circumvented them. Social engineering attacks were also performed against other levels of government in the first period of the Covid19 pandemic (Corona crisis), including a number of Norwegian municipalities [4].

To prevent such attack from succeeding, Gjøvik municipality decided to stop all emails with word, excel and pdf attachments until they could gain control over these type of attacks [5]. By sandboxing these types of attachments, the municipality thereby limited the opportunity-curve as presented by Kowalski in [6] pg. 57 (socio-technical control capabilities over time). However, since the criminal opportunity curve demonstrates that attack methods often out pace control methods it is unclear how this control method will protect Gjøvik municipality, especially if the number of attempts to data breaches will increase in the same rapidly way as it did during the Corona crisis.

In this paper we present the decision made to deal with the social engineering attack method by Gjøvik municipality in a socio-technical context, and further investigate if such controls can lead to a combined crisis management and socio-technical action framework to prevent attacks.

After the introduction we present the background in section 2, before presenting relevant literature in section 3. The research approach is presented in section 4, before presenting the case with interviews and analyzes in section 5. Finally, in section 6, we conclude and suggest future research based on our study.

Proceedings of the 7th International Workshop on Socio-Technical Perspective in IS Development, October 14–15, 2021, Trento, Italia
EMAIL: grethe.ostby@ntnu.no (A. 1); stewart.kowalski@ntnu.no
ORCID: 0000-0002-7541-6233 (A. 1); 0000-0003-3601-8387


## 2. Background

In the Dark numbers survey from 2020 [1], results showed that 28% of the cyberattacks were targeting public administration. The same study found that data breach and hacking still was the most reported attack. In 69% of the incidents, strategic management was involved, and 56% reported that they in the aftermath of the attack had made changes in their policies. However, only 11% reported the attack to the police, despite the police's recommendations to do so [7]. This might be a consequence of the fact that only 44% of the population do not think the police can help them with investigation of such cases [8]. As a number of publicly known cases also are dismissed by the police (e.g. the attack against Helse Sør-Øst [9]), and 40 out of 44 such cases in Oslo in 2016 were dismissed by the Oslo police district [10].

We suggest that since the majority of cases are dismissed by the police there is a need to support competence development for cybersecurity incident management at the municipal level. Additionally, we suggest that the Norwegian laws and regulations on crisis management move the responsibilities away from crime reports and crime handling by the police over to the different organizations (like the municipalities).

> "The Norwegian law concerning the municipality's emergency duty, civilian preparedness and the Civil defense organization outlines the municipality's responsibility to analyze and make emergency preparation based on risk and resilience in their geographical designated area" [11]. "The municipalities would set up prepared societal emergency work that will 1) protect the population and contribute to uphold critical infrastructure, 2) give an overview of knowledge and awareness of societal critical challenges and what effect these challenges would have on the society and communities, 3) reduce risk and vulnerability through preventive work, and 4) ensure good emergency preparedness and crisis contingency" [11].

Moreover, due to the responsibilities outlined above, the municipalities in Norway are mostly self-assurance organizations, that is, they must pay for damages from their own budget. This may also lead to more focus on prevention than if they held normal type of insurance.

For the municipalities to respond to cyber-crime, the understanding of the cyber-attack business is essential. Huang et. al. (2018) outline the cyber-crime business in a value-chain perspective. The primary activities in the mentioned value-chain perspective are 1) vulnerability discovery, 2) exploitation development, 3) exploitation delivery and 4) action, which can be directly translated to the adversary of an incident response process. In this paper we approach the challenges of the cyber-attack business – with an adversary incident response framework combined with a socio-technical analysis framework which take the municipality societal responsibility and challenges into consideration.

## 3. Relevant literature

Crime science has traditionally studied incidents, not persons [13], and has a number of conceptual frameworks like 1) the rational choice perspective, 2) the routine activity approach and 3) the crime patterns theory, which all tries to explain incidents to prevent or control crime and disorder [13]. However, the studies are usually based on target studies, geographical surveys and case studies based on happened incidents, and does not analyze initiated prevention steps with no incident outcome. Additionally, crime science does not often take into consideration how response to crime may minimize the crime outcome. In this paper we therefore suggest to use incident framework like [14] to get a broader approach to crime prevention and crime response and recovery.

Numerous opportunity reducing techniques are suggested in crime science [13]. These opportunities are however systematized to increase effort and risk, to reduce rewards and provocation and to remove excuses [13]. As cyber criminals in addition to targeting private persons also target organizations, several societal, organizational, cultural, methodological, and technical analyses are not taken into consideration in the traditional cyber-crime prevention framework mentioned. In this paper

we therefore suggest a socio-technical analysis framework in combination with the an incident framework.

The "objective of socio-technical design has always been the joint optimization of the social and technical system" [15], and the early motivation for developing socio-technical theories was initiated by the desire to improve industry-workers stationary and repetitive job situation [15]. In this paper our motivation is to close the socio-technical gap in crisis management handling, and to create a framework to support those in the situation of making crisis decisions.

We do not try to create a new socio-technical model, instead we will combine a traditional dynamic socio-technical approach, proposed by Leavitt in 1965 and modified by Kowalski in 1994 [6], [16] with the static Security-by-Consensus model as presented by Kowalski [6] to analyze the case mentioned. Leavitt's model of organizational change comprises four concepts tightly connected to each other – people, task, structure, and technology. The modified Kowalski model also consists of four concepts, culture and structure on the socio site and methods and machines on the technical site. Kowalski's model is presented in figure 1:

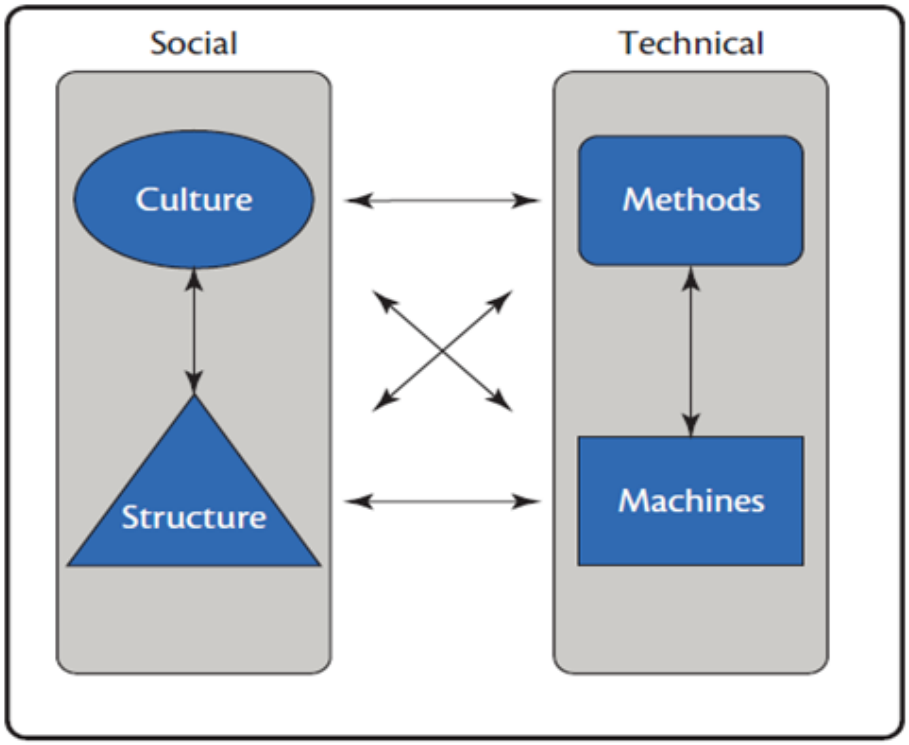



**Fig. 1.** Socio-technical approach [6]

In an organization, there will be several stacks (like in the SBC-model mentioned) to consider when to perform socio-technical analysis. Each of the stacks has it own socio-technical performance [6], and to analyze a case like the one we present in this paper, all stacks would need to be analyzed to find these socio-technical performances. Such a framework was suggested by Kowalski [6], and is presented in figure 2.

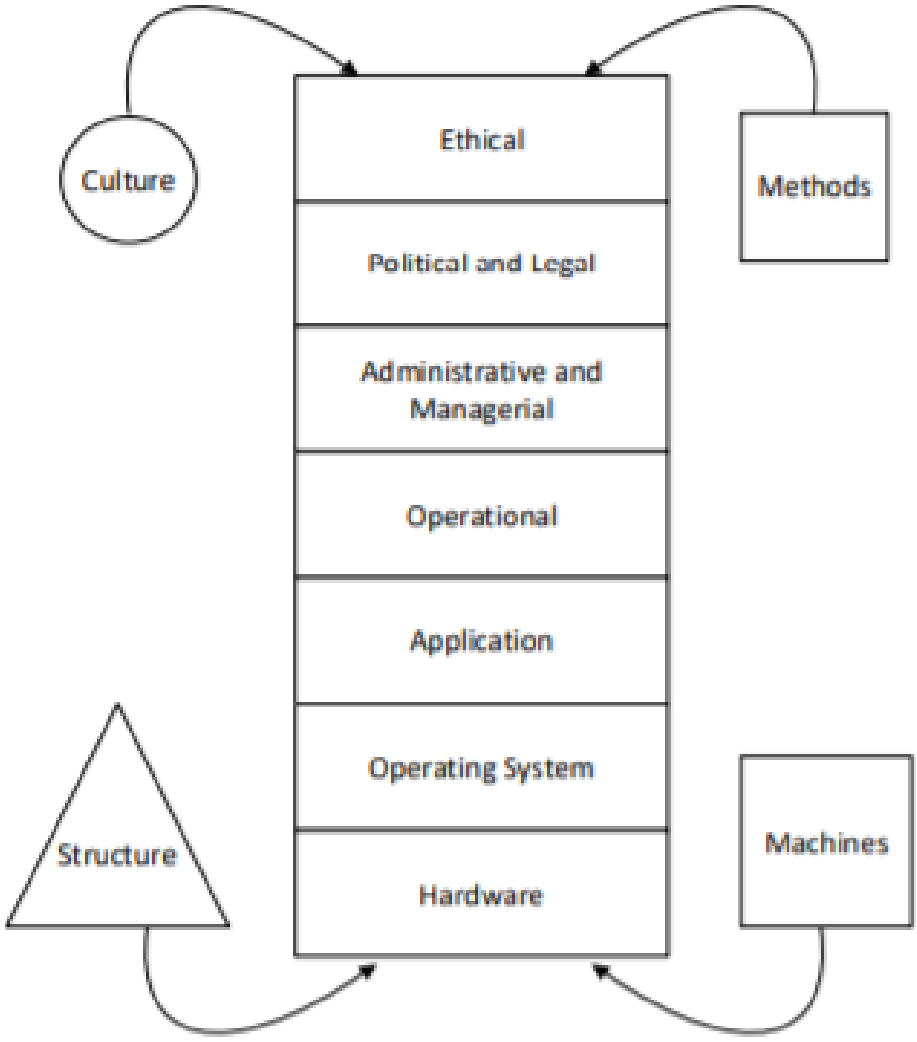



**Fig. 2.** The Security by Consensus model in a socio-technical context [6]

When analyzing the organizations prevention performances in such socio-technical context, we suggest one would need to combine it with the crisis management responsibilities as mentioned in the background. In 1994, Kowalski suggested that this model should be implemented to support a day-to-day emergency response [6]. Kowalski's original suggestion is presented in figure 3.

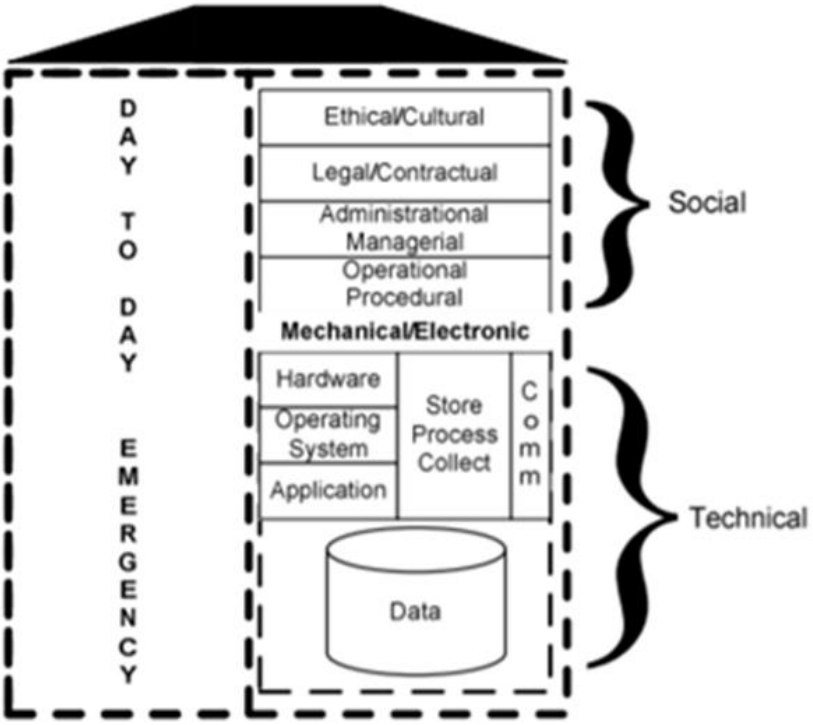



**Fig. 3.** SBC Model suggested to support a day-to-day emergency response [6]

The information shared, escalated, and de-escalated (and adapted) on each layer in this model (figure 3) is in need of being accurate and efficient. Turoff et. al. [17] present a dynamic emergency response management information system to improve information flow. The suggestion is more of a top-down approach, thereby socio-technical semiotics like presented by Piccolo et. al [18] is better for considering information flow in necessary crisis communication. However, Piccolo et. al does not consider the practicalities of what should be considered on which layer in the organizational semiotics. Thereby we suggest using established incident response systems to support information sharing and to have the same information sharing approach on all layers involved in an incident.

In ongoing teaching and research on management at the Norwegian Cyber Range (NCR)/Norwegian University of Science And Technology (NTNU) [19], [20], we are targeting management responsibilities and incident response using the NIST-framework. The American National Institute of Standards and Technology (NIST) provides organizations with a structure for "assessing and improving their ability to prevent, detect and respond to cyber incidents" [14]. The framework consists of 5 stages, 1) Identify, 2) Protect, 3) Detect, 4) Respond and 5) Recover. The framework is presented in figure 4.

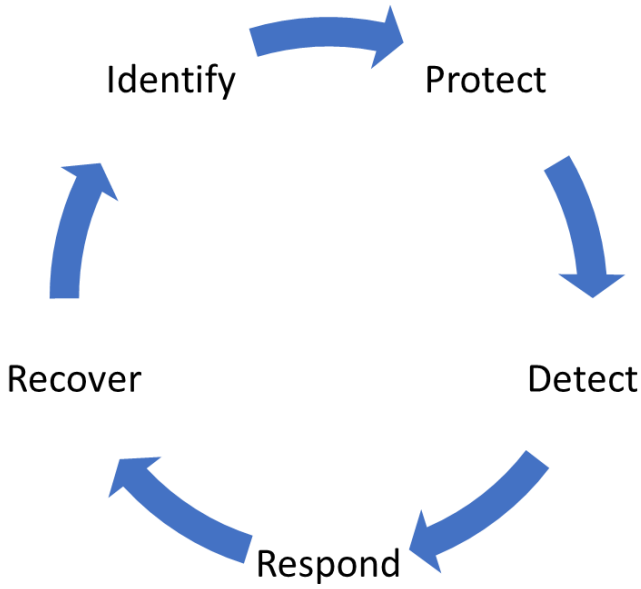



**Fig. 4.** NIST Cyber security framework [14]

By the nature of the case, we present in this paper, we will focus on the identify, the protect and the detect phases of the framework, but also outline the consequences in the respond and the recovery phases.

## 4. Research approach

In this paper, we approach the crime prevention challenge by using the design science research in information systems (DSRIS) [21]. Design science research (DSR) is a methodology which can be conducted when "creating innovations and ideas that define suggestions through the development process of artifacts which can be effectively and efficiently accomplished" [21].

How to work on DSR is presented in a thesis written by G. R. Karokola [22]. He visualized this approach as outlined in figure 5. However, logical formalism in figure 5 is in our research modified with an inductive approach instead of abductive approach used by Karokola.

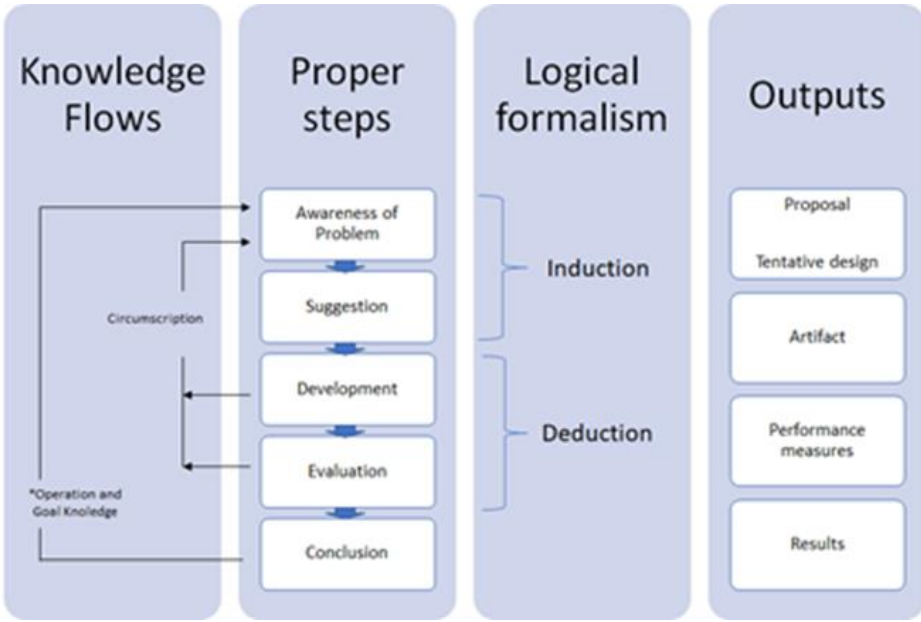



**Fig. 5.** Design research methodology – modified from abduction to induction [22]

As visualized, we have approached the study by what can be referred to as an inductivist approach (instead of abductive or deductive). The inductivist approach starts by first observing a phenomenon and then generalizing about the phenomenon which leads to theories that can be falsified or validated [6]. We have presented the problem by a prevention decision case in Gjøvik Municipality and performed a socio-technical analyze using the SBC model in a socio-technical context (see figure 2) combined with the NIST crisis management framework (see figure 4) to present information from interviews with the decision-makers in Gjøvik municipality. Our suggested combination framework is presented in figure 6.

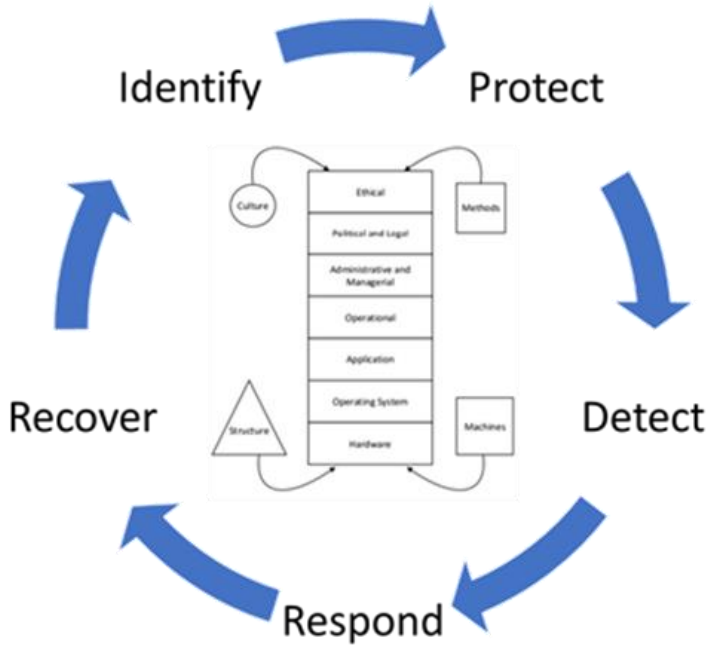



**Fig. 6.** A socio-technical and risk-management root cause analysis framework

We conducted interviews with two of the four people involved in the decision, and the interviews were conducted as open interviews [23] where the participants freely could tell their perception of the situation and decision. We followed up with a few control-questions about crisis management and socio-technical thinking based on what was already told by the participants. Due to integrity issues, no quotes are presented in this paper. The participants were given the possibility of proof-reading the final written case-text to ensure that the content was correct before we started up with our analysis.

As our proposed artifact is a combined risk-management and socio-technical framework to prepare for cyber-attacks, we suggest that this model can be generalized after validation in case-studies in other organizations.

## 5. The case of Gjøvik Municipality prevention decision – a socio-technical and risk-management root cause analysis

After municipalities on the Hedmark-site of the Inland county in Norway was attacked by virus via phishing attack [4], the BAG-group (decision and recommendation group) in the IT-department in Gjøvik Municipality decided to escalate their prevention suggestion to strategic level in the Municipality. The suggestion contained several measures, like 1) to block macros from word, excel and ppt documents, 2) to block internals from sending and receiving emails with word, excel and ppt-files, and 3) to close down all incoming and outgoing emails all together. The suggestion was successfully accepted with immediate effect. The internal blockage lasted for a few days, and the external blockage lasted for proximately 14 days. At this stage no cyber-attacks against the Gjøvik municipality had been discovered.

During the blockade, the municipality implemented sandboxing of word, excel and ppt-files attached to emails, where all the files would be opened and controlled in the sandbox before the email could be passed on.

The IT-department in the municipality participate in a diversity of fora for information security (like Athea[2] and NorCERT[3]) together with amongst others the mentioned municipalities affected by the virus. It was in these fora they were informed about the content of the attacks, and it was the format of the phishing-attack with macros for reuse of internal emails which were analyzed to be the alarming threat. Knowing the internal status on clicking on links the group who decided the measures where confident in their decision (the municipality had already had two phishing attack tests amongst their employees, executed by students from NTNU, where both tests ended up with proximately 10% of the employees clicked on the links in the emails).

The crisis management was not involved in this situation (as the crisis had not yet happened), but the escalation process routine in the municipality was followed: When the IT-department would have to affect the daily routines in the municipality organization, strategic manager in line shall be involved.

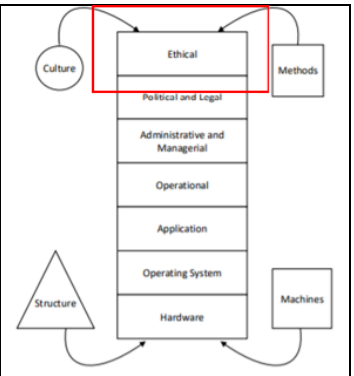
## 5.1. A socio-technical and risk-management root cause analysis framework.

Even though the mitigation measures in Gjøvik municipality first and foremost were executed in the identify and protect phase of a possible data breach, we argue that the consequences in the detect, the respond (e.g. the implementation of the sandbox) and the recover phases were considered. Especially due to the increased number of cyber-attacks during the Corona-crisis. The Corona-crisis itself requires vast crisis management work, and another crisis on top of the ongoing crisis could have affected the organizations capabilities to handle (respond to) the situation, and the recovery could have been very difficult.

In this section we present steps of the combined NIST framework and socio-technical framework presented in figure 6. We have chosen to pesent the Identify-phase of the NIST-framework applied to the socio-technical analyses of the Gjøvik decision in a detailed context (section 5.2) and outline overall importance of similar analyzes for the other NIST-phases in the next sections (section 5.3 – section 5.6).

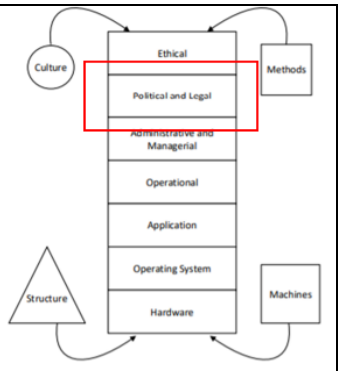
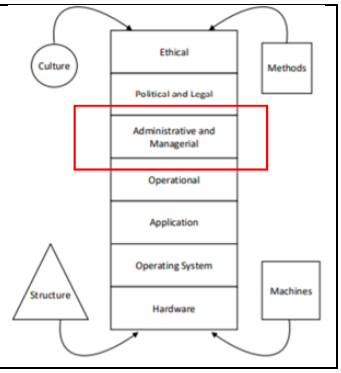
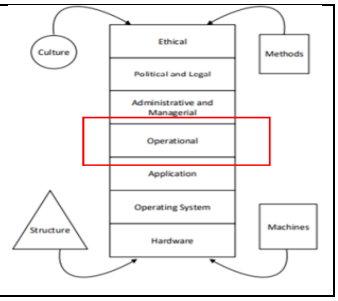
## 5.2. The socio-technical root-cause analysis to IDENTIFY the situation

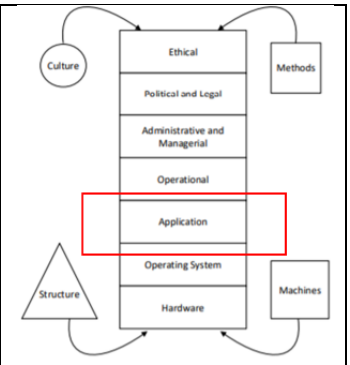
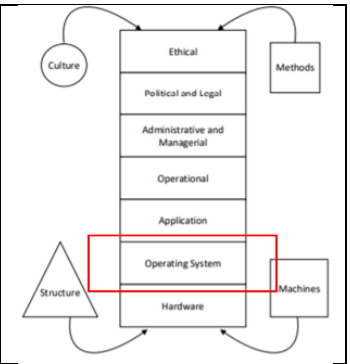
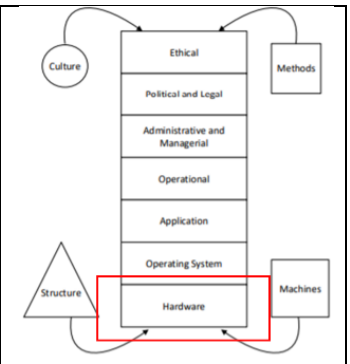
In this section we present the socio-technical analysis (culture, structure, methods, and machines) of each stack in the SBC-framework framework suggested, on how the municipality identified and could identify vulnerabilities in the stacks.

| | |
|---|---|
| There is a strong culture for considering ethical questions in Gjøvik Municipality. In this case, one could have identified that the cost of closing the email-accounts would be too large to do this job, but the internal culture accepted the beneficial arguments to be more important.<br>It could have been identified ethical concerns on the methodology to execute the cut-off, but there were no hidden agendas, and information about the decision was outlined in public (Facebook), which the local newspaper also put forward.<br>The possible draw-back identified on the ethics of the situation was for how long the systems would-be put-on hold. There was no clear timeline on the implementation-phase of the sandboxing in the machines, and thereby important emails to the municipality could have been blocked.<br>One could also question whether the crisis management group should have been involved all together. The decided structure |  |

[2] https://www.atea.no/

[3] https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/

| | |
|---|---|
| for decisions were followed, but due to the high crisis-risk of the decision, one ethical consideration could have been to involve the crisis management. | |
| The political direction in the Norwegian municipalities is put forward every fourth year, and one political priority in Gjøvik municipality is to be a university city, and as the Information security environment in the University is one of the prioritized areas in the University, so it has also become in the municipality. This is proven by the municipality welcoming students to do tests and write studies in the area. The political culture may therefore influence the culture within the organization, and thereby it might have been easier to take the decision.<br>The legal aspect due to the crisis management responsibility suggests that the decision is owned by the municipality and cannot be argued unless the decision is violating any other laws. One may even argue that not taking the decision could have violated the responsibility [24].<br>To implement the sandboxing system would thereby be according to the law mentioned. |  |
| The structure of the escalation routine starts normally at helpdesk if abnormalities occur. The on-duty system responsible would, if necessary, gather the BAG-group, which would consider involving the strategic manager. The strategic manager would eventually consider gathering the crisis management group, and necessary decisions would be taken at the proper stage for the case at hand.<br>One has therefore identified that the culture for escalation is a bottom-up approach, where the operational organization outline recommendations to (in this case) prevent the situation. |  |
| With the bottom-up culture described, a great deal of trust is also put on the operational organization to identify the right decision and execute the decision.<br>Their suggested method was to block emails and macros from files, and when doing so, implement sandboxing before opening the systems again. The implementation was finished within two weeks. |  |

| | |
|---|---|
| As much as the municipality is dependent on using their email-system, word, excel and ppt, they still identified that they have an internal culture in the organization to set aside the applications for this period. This is proven right from the fact that there have not been any public critical comments on the decision. If there has been any internal critique, they also had identified the decision to live with such critique to be right. To make the applications unavailable to the organization may have postponed important necessary written work, but they identified the internal and external structure and culture of information would prevent such critique. |  |
| The operative systems in this situation are well known systems, and the decision they identified to close all macros on these systems would make the applications unavailable for a short amount of time (prox 3 days for the internal users). The same identified issues on culture, methods and structure as described for applications was analyzed, and in this case had the same outcome. |  |
| To protect the hardware from the virus, the identified implementation of sandboxing was essential. The method chosen was suggested from the information security fora's the municipality is a part of. One may therefore say that there is a good culture for collecting knowledge from external expert groups.<br>As previously mentioned, the municipality is self-assured, and this could also be an important impact identified for making the decisions they did. A costly investment in hardware would not have been desired in an already pressured financial situation (because of the Corona-situation). |  |

In the following sections we outline how socio-technical findings would be important in the other stages of the NIST-framework, but we do not go through all stacks in the socio-technical SBC framework.

## 5.3. Update on risk-and resilience analysis to PROTECT from data breaches and hacking

A part of the outlined regulations [25] and municipality guidance's [26], is to regularly update risk- and resilience analysis as a baseline for the emergency (contingency)-plans in the organizations. The organizational structure in the municipalities for update is all set, but the methodology is often to do an update every other year, and thereby cases like the one described in this paper might be forgotten. The

case would be a sub-issue but would have been a good example to use for deciding what culture, structure, methods, and machines would be necessary to protect the organizations from such attacks, using the SBC-model to explain the risks in the different stacks.

## 5.4. Emergency and contingency plans to DETECT similar data breaches and hacking

In the municipality guidance [27], it is suggested to have emergency and contingency plans on both strategic and sectoral levels in the organization. For the municipality IT-department, it would be wise to do a socio-technical analysis as described on a diversity of Information security issues (like those described in [1]), and make relevant emergency and contingency plans relevant for all issues.

## 5.5. RESPOND to data breaches and hacking

The respond to and escalation in an attack as described would vary by the severity of the attack, but like in the Hedmark-municipalities situation [4], managing the Corona-situation was already heavily burdening the municipalities crisis management team, and they were concerned that the impact of simultaneous crisis was emerging, and also ethical considerations were necessary to consider. Even political priorities were under discussion in the situation mentioned. Information from the Information security fora could also have been relevant to prepare for handling such situations, and in this case, it could be an important foundation for the decision Gjøvik made.

## 5.6. Update on Information security policy in RECOVERY phase data breaches and hacking

In a situation with several ongoing crises at the same time, the recovery phase can take more time than usual. To use time on recovery from such a situation and do the proper socio-technical analyzes as suggested in this paper, could take too much time from other ongoing crises, and could be set aside (and forgotten) before the next crisis occurs. It would therefore be important to establish the framework as part of the deviation report, to be able to collect the analyzes for later recovery [6, chap. 13].

## 6. Conclusion and future research

In this paper we have discussed the Gjøvik Municipality decision case in a combined socio-technical and risk-management root cause analysis framework. We suggest that the combination of the two frameworks (the SBC-model/Kowalski model and the NIST-framework) outline first and foremost a good analysis framework to prevent data breaches and hacking from happening, but also to be able to prepare for the respond and the recovery phases. Our plan is to invite other municipalities in testing the framework, to see what impact such framework could have on incident management in organizations affected by such attacks.

We have only tested the SBC-model combined with the Kowalski-model, as part of the socio-technical analyses. One may suggest that other socio-technical models could be more suitable in combination with the NIST-framework, and such could be tested to validate and possibly figure out the reliability of our suggested framework. Other incident response frameworks than the NIST-framework might also be relevant to test for combination with socio-technical models, and this needs to be further tested in other studies. First however, we need to test if our suggested model in this paper can be applicable in other case-studies.

Organizational semiotics are argued out of this paper but are suggested to have a great impact on emergency responses. Mentioned dynamic emergency response management information system (DERMIS) like presented by [17], and a socio-technical semiotic approach to build community resilience, like presented by [18] will be an important part of the future test and research of combining socio-technical and incident response tools.

## 7. Acknowledgements

We would like to give our special thanks to Gjøvik municipality, which gave us the possibility to do interviews with involved parties in the decision. Our plan was to interview relevant parties on both strategic, tactical, and operational levels in the organization, but the tactical head of the IT-department was disabled from participating. We would, however, give our special thanks to the participant from the strategic management group and the participant from the operational IT-department and member of the BAG-group, for being able to participate in interviews in a hectically period of the Corona-crisis situation.

## 8. References

[1] The Norwegian Business and Industry Security Council, "The dark numbers survey 2020," 2020.
[2] T. Bie, "Stortinget hacket: – Krise," *ITAVISEN*, 2020.
[3] J. Gilbrandt and M. Rønning, "Omfattende IT-angrep mot Stortinget," *dagbladet.no*, 2020.
[4] A. Krantz, M. F. Børresen, T. I. Hagen, and A.-K. Mo, "Dataangrepet: Kan skade korona-beredskapen," *nrk.no*, 02-Sep-2020.
[5] M. B. Staveli, "Gjøvik stopper e-poster med vedlegg etter hackingskandalen," *oa.no*, 2020.
[6] S. Kowalski, "IT Insecurity: A Multi-disiplinary Inquiry," Stockholm University, 1994.
[7] Politiet, "Datakriminalitet," *www.politiet.no*, 2020. [Online]. Available: https://www.politiet.no/rad/datakriminalitet/. [Accessed: 14-Nov-2020].
[8] NorSIS, "Nordmenn og digital sikkerhetskultur 2019," 2019.
[9] Digi.no, "Henlegger saken om dataangrepet mot Helse sør-øst," *digi.no*, 05-Dec-2018.
[10] R. A. Njie, "Kripos advarer: – Stor økning i datakriminalitet," *nrk.no*, 03-Apr-2017.
[11] G. Østby and B. Katt, "Cyber Crisis Management Roles – A Municipality Responsibility Case Study," in *Science and Technology in Disaster Risk Reduction in Asia*, 2019, pp. 168–181.
[12] K. Huang, M. Siegel, and S. Madnick, "Systematically Understanding the Cyber Attack Business: A survey," *ACM Comput. Surv.*, vol. 51, no. 4, p. 36, 2018.
[13] P. Hartel, M. Junger, and R. Wieringa, "Cyber-crime Science = Crime Science + Information Security," *Inf. Secur.*, pp. 1–55, 2011.
[14] K. Scarfone, T. Grance, and K. Masone, "Computer Security Incident Handling Guide," 2008.
[15] E. Mumford, "The story of socio-technical design: Reflections on its successes, failures and potential," *Information Systems Journal*. 2006.
[16] H. Leavitt, "Applying Organizational Change in Industry: Structural, Technological, and Humanistic Approaches.," in *Handbook of organizations*, J. G. March, Ed. 1965, pp. 1144–1170.
[17] M. Turoff, M. Chumer, B. Van de Walle, and X. Yao, "The design of a Dynamic Emergency Response Management Information System," *J. Inf. Technol. THEORY Appl.*, vol. 1, no. 1, pp. 253–292, 2012.
[18] L. Piccolo, K. Meesters, and S. Roberts, "Building a Socio-technical Perspective of Community Resilience with a Semiotic Approach," *Proc. 18th Int. Conf. Informatics Semiot. Organ.*, vol. 527, 2018.
[19] NTNU, "The Norwegian Cyber Range," 2019. [Online]. Available: https://www.ntnu.no/ncr.
[20] NTNU, "IMT4115 - Introduction to Information Security Management," 2021. [Online].

Available: https://www.ntnu.edu/studies/courses/IMT4115/2021/1#tab=omEmnet.
[21] W. Kuechler and V. Vaishnavi, “A Framework for Theory Development in Design Science Research: Multiple Perspectives,” 2012.
[22] G. R. Karokola, “A framework for Securing a-Government Services, The case of Tanzania,” Stockholm University, 2012.
[23] D. L. Driscoll, “Introduction to Primary Research: Observations, Surveys, and Interviews,” in *Writing Spaces: Readings on Writing*, 2011, pp. 152–174.
[24] Justis- og beredskapsdepartementet, “Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (sivilbeskyttelsesloven).” Norwegian Government, 2010.
[25] Norwegian government, *FOR-2011-08-22-894*. Norwegian Government, 2011.
[26] DSB, *Guidance to holistic risk and vulnerability assessment in the municipality*. DSB, 2019.
[27] DSB, *Municipality guidance, emergency duty*. 2017.

Publication 2

Østby, Grethe; Kowalski, Stewart James; Katt, Basel. (2020) Towards a Maturity Improvement Process – Systemically Closing the Socio-Technical Gap. *CEUR Workshop Proceedings. vol. 2789.*

# Towards a Maturity Improvement Process – Systemically Closing the Socio-Technical Gap

Grethe Østby[a], Stewart James Kowalski[a] and Basel Katt[a]

[a] *Norwegian University of Science and Technology, Teknologivegen 22, 2819 GJØVIK, Norway*

**Abstract**

In this paper we present ongoing research into escalation maturity measurements of organizations. We outline how to integrate a socio-technical approach and LIFT-methodology to improve the escalation maturity improvement process. We suggest this approach can help to close the socio-technical gap in information (cyber) security, and plan to test our ideas on relevant public organizations. Our suggested process consists of three phases, the maturity modelling itself with the analysis of the results, the destination acceptance to define the acceptable level and define the action strategy, and finally the implementation phase with the plan and use of learning methods to apply the strategy. We suggest that an ongoing evaluation of the process must be outlined, to validate the effect of the improvement action points suggested.

**Keywords 1**

Maturity modelling. Maturity improvement. Socio-technical adaption. Socio-technical balance. LIFT-methodology.

## 1. Introduction

The "objective of socio-technical design has always been the joint optimization of the social and technical system" [1], and the early history of developing socio-technical theories started with observations of workers under difficult job-conditions with the motivation to improve their woek situation [1]. Studies have shown that with many information (cyber) security problems only 26% of the issues can be addressed by technology solutions alone [2] Consequently the focus of our research is to examine how the combination of social and technical solutions can be combined and optimized to improve the information and cyber security posture of organizations.

In a recent study at the Inland Hospital trust in Norway the escalation maturity modelling to understand level of maturity in the organization was tested [3]. The study concluded among other things, that the best use of the maturity model is to test maturity on both strategic, tactical and operational levels in the organization, and then next to outline a process for the alignment between these three tiers. The study also suggested future research for an improvement maturity process, which can be used for preparation for improvement-instructions. In this paper we discuss further development of the maturity model tested at the Inland hospital trust in Norway and suggest improvement to maturity improvement framework.

Wahlgren and Kowalski escalation maturity model gives an overview of what should be done within each maturity attribute (as a part of the individual report), to improve the situation [4]. The scores consist of five different scale varying from Non-existent to Optimized maturity on the same attributes, and each score on each level and attribute give overall suggestions for improvement The Østby and Katt study results indicated that it will be important to divide program and action points between the different tiers [3], and in this paper we suggest that both socio and technical action points should be

Proceedings of the 6th International Workshop on Socio-Technical Perspective in IS Development (STPIS 2020), June 08–09, 2020
EMAIL: grethe.ostby@ntnu.no (A. 1); stewart.kowalski@ntnu.no (A. 2); basel.katt@ntnu.no (A. 3)
ORCID: 0000-0002-7541-6233 (A. 1); 0000-0003-3601-8387 (A. 2); 0000-0002-0177-9496 (A. 3)


considered at each level of each attribute for all the tiers in the organizations to support closing the socio-technical gap.

In this paper, we suggest combining a socio-technical MRD-IMC approach [5] to prioritize attributes to balance the socio-technical system, a lift-methodology [6] to fill the socio-technical gap one or two steps at a time and not all at once, and also use the learning processes to make incremental changes in an organization so as to improve systematic and permit adoption of information (cyber) security.

After this introduction we present background and relevant literature in section 2 and 3, before presenting our research approach in section 4. Our proposed model is presented in section 5, and our conclusion and suggested future research are present-ed in section 6.

## 2. Background

The genesis of this study started at the Inland Hospital Trust in Norway. Hospitals in Norway use EMRAM Electronic Medical Record Adoption Model to measure the level of technological efficiency and need of security. EMRAM was established in the USA in 2005 and more than 5000 American hospitals are measured by this system [7]. HIMSS Analytics Europe developed a European standard for the model (HIMSS, 2020), and that model for measuring efficiency is the one used by Norwegian hospitals. The different layers describe how technology- efficient the hospital is, and then what responsibility is needed on the different layers. The higher up on the EMRAM levels the hospital is, a greater degree of employee responsibility is added. The [9] model is presented in figure 1.

| | |
|---|---|
| 7 | Complete EMR; External HIE; Data Analytics, Governance, Disaster Recovery, Privacy and Security |
| 6 | Technology Enabled Medication, Blood Products and Human Milk Administration; Risk Reporting; Full CDS |
| 5 | Physician documentation using structured templates; Intrusion/Device Protection |
| 4 | CPOE with CDS; Nursing and Allied Health Documentation; Basic Business Continuity |
| 3 | Nursing and Allied Health Documentation; eMAR; Role-Based Security |
| 2 | CDR; Internal Interoperability; Basic Security |
| 1 | Ancillaries – Laboratory, Pharmacy, and Radiology/Cardiology Information systems; PACS; Digital non-DICOM image management |
| 0 | All three ancillaries not installed |

**Figure 1.** EMRAM [9]

The problem with this model is that from level 3 and upwards when more responsibilities are added (as this measurement is focused on system security in first and is measured from a system-security perspective), that these added responsibilities do not necessarily correspond to the organizational increased maturity levels.

In a study presented by Wahlgren and Kowalski [10] they tried a slightly different approach for measurement, which focuses more on organizational and administrative aspects of information security aligned with the ISO standard 27005 for Risk processes, and the NIST escalation tier model. In that study the results suggest that IT Security Risk Management Framework can exist at each organizational level. In a complementary study by Wahlgren and Kowalski [11], they tested their maturity model [4] developed to measure a diversity of information security attributes based on the [12] maturity model, but adapted around escalation of IT-related security incidents. Østby & Katt [3] used the systems developed by Wahlgren and Kowalski, and tested their model at both strategic, tactical and operational levels at the Inland hospital trust in Norway.

The results presented in [3], vary on strategic, tactical and operational levels in the organization. Figure 2 outlines the result in histogram form. The results from the strategic participants showed little variance within the group, but clearly showed a need for improvement on all measured attributes, even on organizational structure, though this attribute had the best results. The results from the tactical managers were also aligned within the group. The maturity levels themselves were lower on most attributes. Non-existent results on responsibility, knowledge and education and procedures, gave us signals about major gaps in these areas. Be aware that the figure on the tactical level gives a shortened level axis. The results on the operational level are slightly higher than on the other 2 tiers. The variance within this tier is however larger, with knowledge and education being measured as the lowest attribute in this group. The results from the different levels are presented in figure 2.

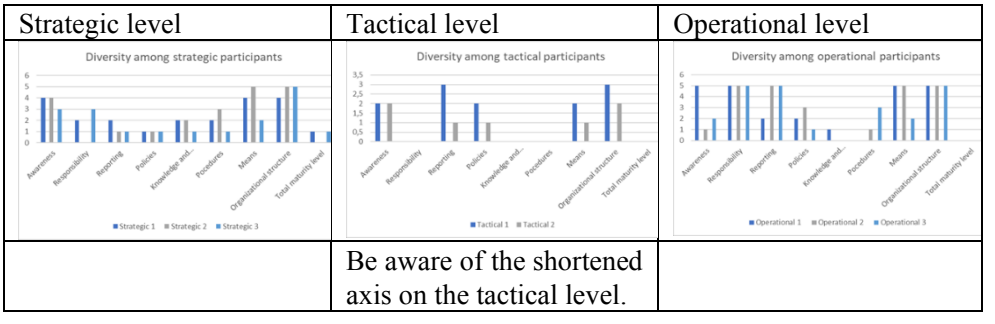



**Figure 2.** Maturity results on strategic, tactical and operational levels [3]

We argue that it would be difficult to fill all the gaps at all levels at the same time, and we suggest that to improve the process and diminish the gaps it is best to start with socio-technical action points on each layer for each attribute. In [13], they suggest using the maturity study as a starting point to design scenarios and exercises for the organizations to learn about the consequence of the current misalignment and also test possible improvement options in a cyber range. In the same paper they also suggest giving input on improvement work in lectures provided for the organizations attending exercises. In this paper, we investigate a variety of information security improvement work and suggest a step-by-step improvement process that can be taught and implemented as a part of the lectures taught and trained at the exercises mentioned. And, as an aftermath of the exercises a reexamination of the decided action points can be followed up using action research in the organizations with the motivation to see what works and at what tier, level and attribute.

## 3. Relevant literature

A successful story on maturity improvement is presented at the NIST-framework webpage [14]. The story presents how The University of Chicago's Biological Sciences Division (BSD) used the NIST-framework to measure and improve their maturity combined with customized tier definitions and a heat-map. This process is presented in figure 3.

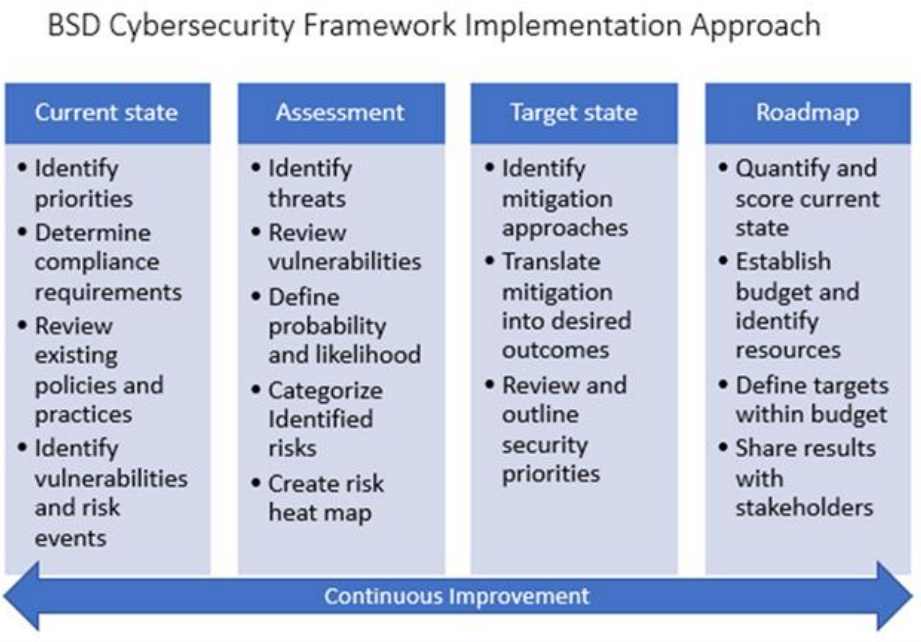



**Figure 3.** NIST improvement process in Chicago BSD work [14]

However, in a case like the hospital-trust case, the roadmap to identify resources may be too overwhelming, and the target state might be too difficult to define without a proper step-by-step approach. It could also be unclear what and how to get the best targets to achieve an adequate socio-technical balance in the organization. That is, if the culture, structure, methods and machines are considered equally, as presented in [15].

In this paper we do not try to create a new socio-technical model, instead we will use a traditional socio-technical approach, proposed by Leavitt in 1965 and modified by Kowalski in 1994 [15], [16]. Leavitt's model of organizational change comprises four concepts tightly connected to each other – people, task, structure, and technology. The modified Kowalski model is presented in figure 4:

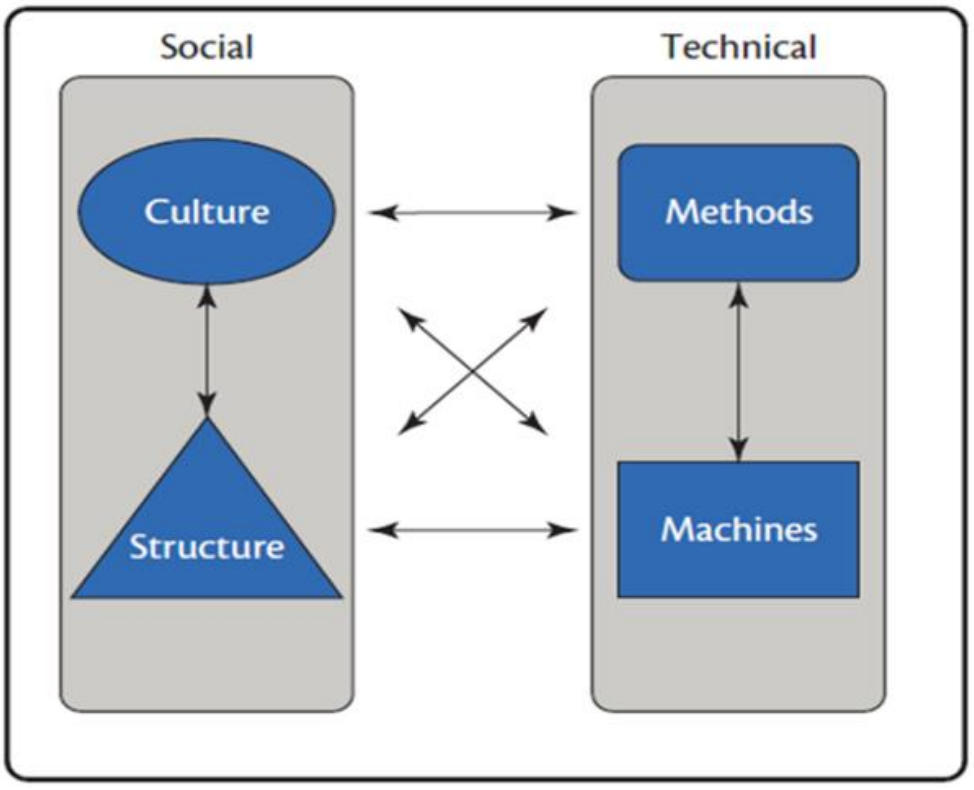



**Figure 4.** Socio-technical approach [15]

At the Carnegie Mellon University, Alberts et al. [5] developed a socio-technical Mission Risk Diagnostic for Incident Management Capabilities (MDR-IMC) to "evaluate a set of systemic risk factors (called drivers) to aggregate decision-making data and provide decision makers with a benchmark of an IM function's current state". Alberts et al. [5] MRD-IMC approach comprises three core tasks, 1) Identify the mission and objective(s), 2) Identify drivers and 3) Analyze drivers. After identifying a "driver profile" (similar to EMRAM and Wahlgren & Kowalski's maturity study), they apply the MDR-IMC approach with systematized driver questions for all the attributes discovered in the "driver profile". The driver questions not only cover how to improve, but also identifying questions on what can be handled by expert-groups, questions on cost-benefit etc.. However, the driver-questions are focused on needs in the organization and not knowledge-based improvement steps. That is, what do you most need to do first for security reasons, instead of what are the ideal steps to follow to expand the knowledge base of the organization to follow.

A well-known improvement process used in Norwegian organizations is the "LØFT-metodikk" developed by [6]. LØFT in Norwegian is a shortcoming of focus on solutions to improve. LØFT itself means "lift up", and consequently we have used LIFT as the English substitute in this paper. LIFT-methodology can be compared with Appreciative Inquiry, which allows individuals to generate something beyond espoused theory and an appreciative inquiry approach to leader development [17]. Hart, Conklin and Allen suggest an appreciative inquiry approach to leader development as presented in figure 5.

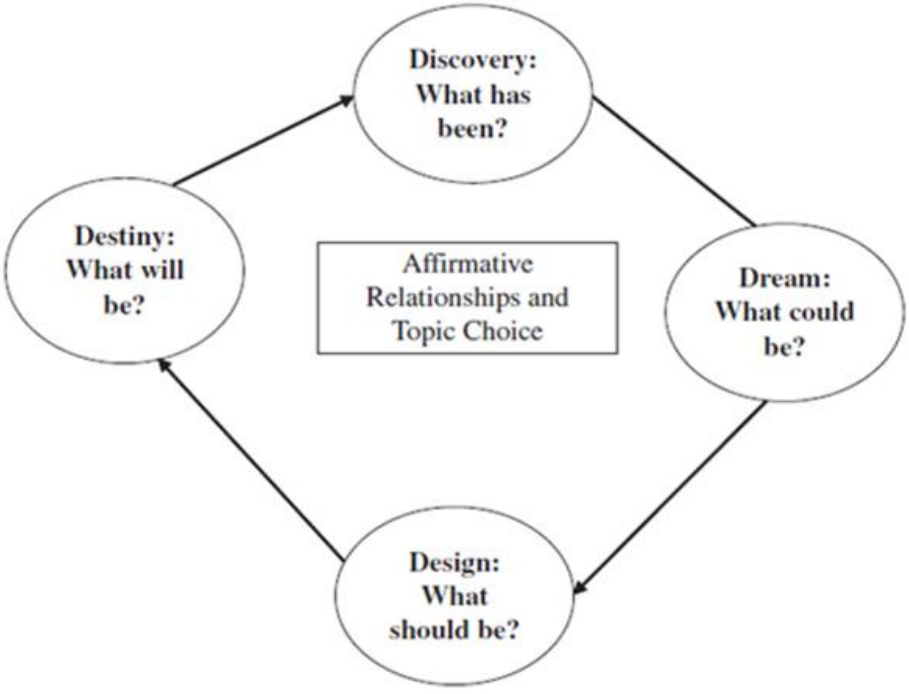



**Figure 5.** Appreciative inquiry approach to leader development [17].

LIFT-methodology is an alternative problem-solving methodology, which focuses on what makes a day acceptable, and ways to get there. Contrary to the more traditional approach used in e.g. surgeries, of which the problem needs to be diagnosed, causes need to be mapped and the pain must be removed [18]. European Brief Therapy Association (EBTA) is doing surveillance on relevant research on the topic, and Dr. Alasdair Macdonald (www.solutionsdoc.co.uk) has done related research available on his website, together with the protocol from EBTA.

In her book about LIFT-methodology for leaders, Langslet recommends some adjustments to the different stages based on the appreciative inquiry model [6]. First, to be careful about problematizing the "what has been". She suggests this can lead to reinforcement of the problem situation. Second, a "dream" might be too ambitious, and that the focus instead should be what is good enough. The LIFT methodology also tries to combine "what should" be with "what will be" to meet the actual organizational requirements, to see where the organization is heading and how to get up to a required level.

Langslet's LIFT-methodology requires knowledge on what would be required to improve one step by step. In our situation, and as presented in the NIST-improvement process, we may know a number of efforts that could close some of the socio-technical gap, but not which ones that can take us from level 5 to level 6 on the specific attribute. Ackerman suggests that the socio-technical gap is "the divide between what we know we must support socially and what we can support technically" [19]. Thereby, the improvement-steps must also consider both social and technical efforts. Additionally Ackerman [19] suggests that palliatives like ideology, politics and education in both socio and technical manners, may affect the capability to close the socio-technical gap. In this paper we target the educational palliative, and in [13] a relevant educational model based on modified backward design is presented. The model is modified with a socio-technical context to close the gap. The modified backward design model does not take into consideration learning methods for different roles/functions when implementing action points, and in this paper, we address this issue with a variety of already developed learning methods to be used in the implementation phase.

## 4. Research approach

In this paper, we approach the maturity improvement challenges, using what can be referred to as a naive inductivist approach. The naive inductivist approach starts by first observing a phenomenon and then generalizing the phenomenon which leads to theories that can be falsified or validated [15]. This approach will use the methodology outlined by design science research in information systems (DSRIS) [20]. This methodology uses artefact design and construction (learning through building) to generate new knowledge and insights into a class of problems.

DSRIS requires three general activities: (1) construction of an artefact where construction is informed either by practice-based insight or theory, (2) the gathering of data on the functional performance of the artefact (i.e., evaluation), and (3) reflection on the construction process and on the implications the gathered data (from activity (2)) have for the artefact informing insight(s) or theory(s) [20].

Karokola [21] suggested a model on how to work on these steps. This model is presented in figure 6. As we are approaching our work in a naive inductivist approach, we modified the logical formalism in the model from abduction to induction.

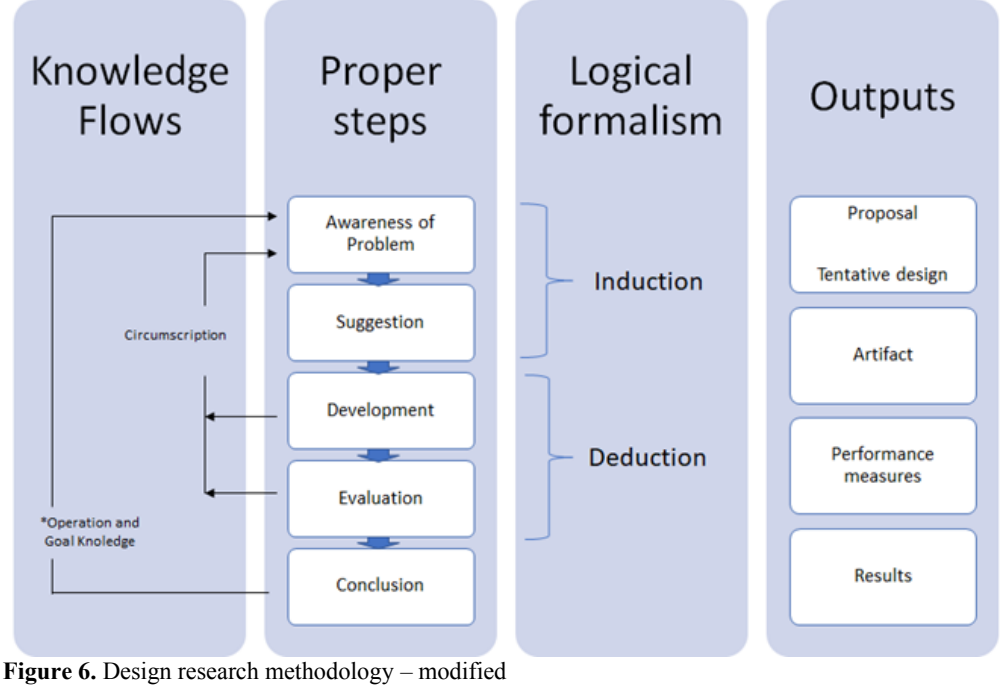



**Figure 6.** Design research methodology – modified

In this research we discuss further development of the maturity model tested at the Inland hospital trust in Norway and suggest a maturity improvement framework (third and fourth step in the 2nd column). That is, as we already have tested the Wahlgren & Kowalski model and evaluated that, we mostly focus on the development phase.

The goal of this paper is therefore to outline our research agenda to develop and improve escalation maturity results. We are currently planning to run trail exercises on Inland hospital trust. We want to focus on how this improvement framework can be employed in improving an organization to transform lessons identified in cyber ranges exercise to lessons learned in daily operations. We want to answer the questions by focusing on how improvement systems can be employed in improving maturity in the organizations tested, and if our model is approved by the STPIS-community, we will test our suggestions through action research at the Inland hospital trust.

## 5. Maturity improvement – a socio-technical lessons learned approach

In this paper we suggest a maturity improvement process on Information (cyber) security in organizations, taken into consideration the socio-technical gap, but also considering how learning processes can be used to support a step-by-step improvement process, and what each step of improvement consists of in a socio-technical context. Our suggested process is presented in figure 7.

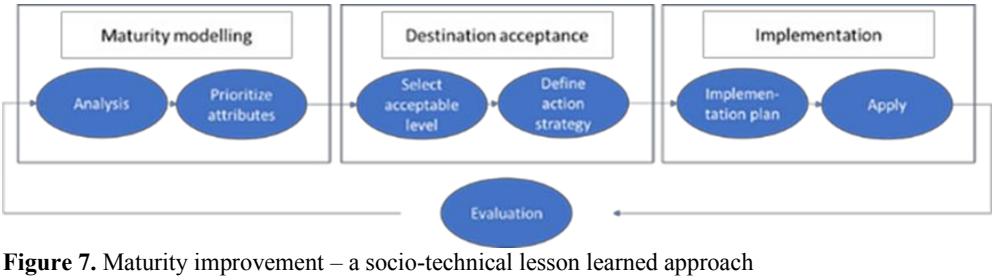



**Figure 7.** Maturity improvement – a socio-technical lesson learned approach

In the first step, called maturity modelling, we suggest after executing the maturity-study [3], [4], to analyze the results based on Alberts [5] drivers, to identify the mission and objective(s), to be able to prioritize attributes for improvement. However, we suggest more granularly improvement-suggestions to be able to measure what improvement-suggestions give what effect, and on which layer (measure) they are most suitable. This suggestion is presented in figure 8 (we have used the Initial step on Awareness from Wahlgren and Kowalski [11] as our example).

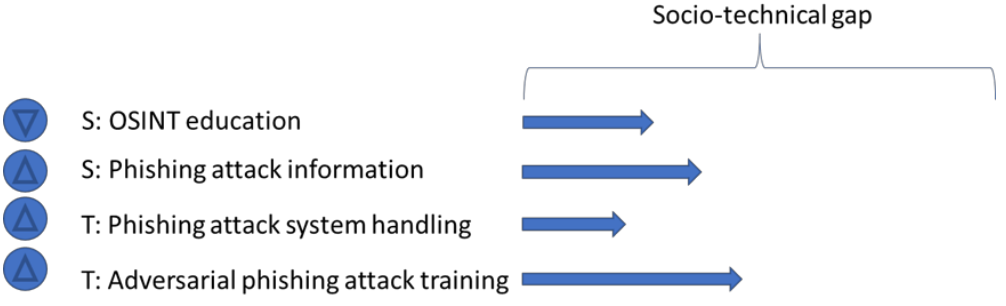



**Figure 8.** Granular suggestions effect on closing the socio-technical gap

In figure 8, a variety of social (S) and technical (T) (as presented in figure 4) improvements in one layer (measure) in one attribute is suggested (in our case Initial Awareness), and the effects are presented under the socio-technical gap. On the left side of the figure arrows up and down are presented to be able to test and vary whether these suggestions are best suited at the chosen layer (Initial) or if they are better suited in the layer above or under.

In the second step, called destination acceptance, we suggest using the LIFT-methodology to first figure out what is an acceptable level for each tier in the organization (strategic, tactical and operational), then to suggest what to do to get to that level. The different levels are already defined on each question in the questionnaire, from non-existent to optimized, and we suggest that the model's suggestions need to be refined in concrete design by using LIFT-methodology.

LIFT-methodology does have some weaknesses, because there might be regulations that require what is acceptable in information security, not what is "good enough". Still, if the requirements are to be managed, LIFT can be used to get from non-existent to Optimized step by step. In this case the

presented suggestions could be divided and concretized for each step and based on what is presented in figure 8. We present this approach in figure 9 (using the awareness attribute).

| | Attribute: Awareness | Action points: From non-existent to optimized (examples) |
|---|---|---|
| Non-existent | Increase awareness of employees through courses of various kinds on IT-related security and privacy incidents and threats. | |
| Initial | Inform employees which consequences various IT-related security and privacy incidents may have. | S: OSINT education<br>S: Phishing attack information<br>T: Phishing attack system handling<br>T: Adversarial phishing attack systems |
| Repeatable | Inform employees which security measures to be applied if various IT-related security and privacy incidents occur. | |
| Defined | Make sure that the information on various IT-related security and privacy incidents and their consequences are routinely updated and that the update is accepted by the organization. | |
| Managed | Make sure that the information on various IT-related security and privacy incidents and their consequences are continuously evaluated and, if necessary, improved. | |
| Optimized | | |

**Figure 9.** Successfully information security action points previously done on awareness attributes to enhance from one level to the next.

To explain what we have done in figure 9, we may use the example from figure 8 – the Initial level. We suggest searching for what is done today, what is successfully done other places, and what would be the acceptable approach to get to the next level. In our example (the Initial level in figure 9), we would have used suggestions as presented in figure 8.

We suggest presenting a prioritization to the management board of which will select acceptable levels. When prioritized, an action strategy must be defined within the regulations of economy and project management (cost/benefit analysis) in the organization.

In the third step, called implementation, we suggest how to implement the projects. As mentioned in or model-analysis, we suggest implementing plans at acceptable levels, with combined socio-technical action points. When acceptable levels are decided, implementation should be applied step by step by either or both microlearning methods [22], organizational learning methods [23] and institutional learning methods [24]. This process is presented in figure 10.

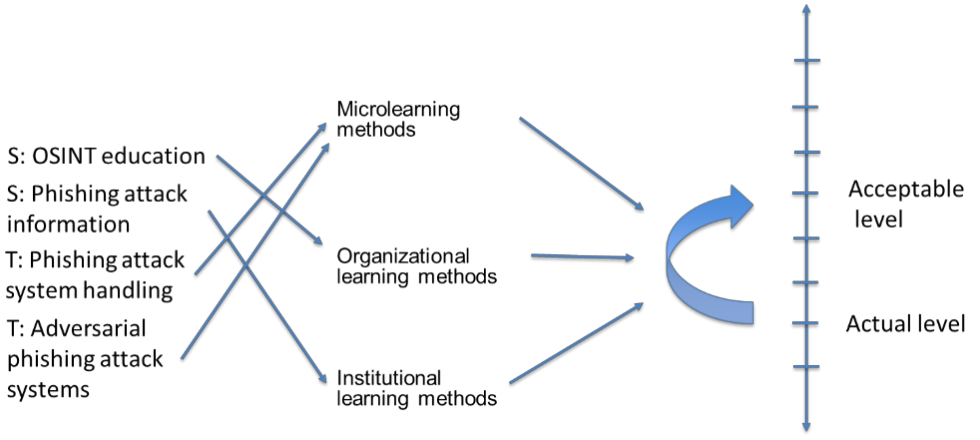



**Figure 10.** Implement processes to learn action points

In figure 10 we suggest how the action points presented in figure 9 can be implemented by choosing learning methods suitable for that particular action point. This may vary from organization to organization and would be necessary to decide before most implementations.

Finally, we suggest an ongoing evaluation of the process, to validate the effect of the improvement action points suggested.

## 6. Conclusion and future work

In this paper we present a maturity improvement process using MRD-IMC approach, LIFT-methodology, and the learning methods in a combined Maturity improvement process - a socio-technical lesson learned approach. We suggest that this process applies best practice for using escalation maturity models to raise and educate cyber security maturity from one level to a better level.

After this framework has been reviewed by the research community at the STPIS 2020 we wish to test the relevance of our framework in different management groups in Norwegian public sector to develop and evaluate our suggestions to provide cyber security improvement work that will enhance the cyber security maturity.

After we have tested the suggested improvement process in the health care services, we want to test the process also into other private and public sectors.

## 7. References

[1] E. Mumford, "The story of socio-technical design: Reflections on its successes, failures and potential," *Information Systems Journal*. 2006.
[2] Cisco, "Annual cyber security report," 2018.
[3] G. Østby and B. Katt, "Maturity modelling to prepare for cyber crisis escalation and management," 2019.
[4] G. Wahlgren and S. Kowalski, "A Maturity Model for Measuring Organizations Escalation Capability of IT-related Security Incidents in Sweden," *Assos. Inf. Syst.*, 2016.
[5] C. Alberts, A. Dorofee, R. Ruefle, and M. Zajicek, "An Introduction to the Mission Risk Diagnostic for Incident Management Capabilities (MRD-IMC) CERT ® Division," 2014.
[6] G. J. Langslet, *Løft for ledere*. Gyldendal Norsk forlag, 2003.
[7] B. Monegain, "Two health systems awarded Stage 7," *Healthcare IT news*, 2012.
[8] HIMSS, "ELECTRONIC MEDICAL RECORD ADOPTION MODEL (EMRAM)." [Online].

Available: https://www.himssanalytics.org/europe/electronic-medical-record-adoption-model. [Accessed: 15-Sep-2020].
[9] T. Himss and A. Emram, "EMRAM," *HIMSS Analytics*. HiMSS Analytics, 2017.
[10] G. Wahlgren and S. Kowalski, "IT Security Risk Management Model for Cloud Computing," *Int. J. E-entrepreneursh. Innov.*, vol. 4, no. 4, pp. 1–19, May 2014.
[11] G. Wahlgren and S. Kowalski, "A Maturity Model for IT-Related Security Incident Management," in *Business information systems*, Springer, Cham, 2019.
[12] ISACA, "The risk IT framework," 2009. [Online]. Available: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx.
[13] G. Østby and S. Kowalski, "Preparing for Cyber Crisis Management Exercises," in *Augmented Cognition*, 2020.
[14] NIST, "Uses and Benefits of the Framework," *NIST Cybersecurity framweork web-page*, 2020. [Online]. Available: https://www.nist.gov/cyberframework/online-learning/uses-and-benefits-framework?campaignid=70161000001Cs1OAAS&vid=2117383.
[15] S. Kowalski, "IT Insecurity: A Multi-disiplinary Inquiry," Stockholm University, 1994.
[16] H. Leavitt, "No Title," in *Handbook of organizations*, 1965, pp. 1144–1170.
[17] R. Kaye Hart, T. A. Conklin, and S. J. Allen, "Individual Leader Development: An Appreciative Inquiry Approach," *Adv. Dev. Hum. Resour.*, vol. 10, no. 5, pp. 632–650, 2008.
[18] S. Hansche, "Designing a security awareness program: Part 1," *Inf. Syst. Secur.*, 2001.
[19] M. S. Ackerman, "Intellectual challenge of CSCW: the gap between social requirements and technical feasibility," *Human-Computer Interact.*, vol. 15, no. 2–3, pp. 179–203, 2000.
[20] W. Kuechler and V. Vaishnavi, "A Framework for Theory Development in Design Science Research: Multiple Perspectives," 2012.
[21] G. R. Karokola, "A framework for Securing a-Government Services, The case of Tanzania," Stockholm University, 2012.
[22] I. Buchem and H. Hamelmann, "Microlearning: a strategy for ongoing professional development," 2010.
[23] K. E. Weick, "The Nontraditional Quality of Organizational Learning," 1991.
[24] J. Watts *et al.*, "ILAC Working Paper 3 Institutional Learning and Change: An Introduction," 2007.

Publication 3

Østby, Grethe; Kowalski, Stewart James. (2022) ORGANIZATIONAL LEARNING WITH CRISES. *EDULEARN22 Proceedings.* Iated.

# ORGANIZATIONAL LEARNING WITH CRISES – TRIPLE LOOP LEARNING IN CYBER SECURITY EXERCISES

**Grethe Østby, Stewart James Kowalski**

*Norwegian University of Science and Technology (NORWAY)*

## Abstract

In this paper we present our ongoing attempts to introduce and develop a triple-loop learning process via a discussion exercise in a Master of Science (MSc) introduction to information security management course. Over a two years period (course semesters of 2020 and 2021), we have tested a discussion exercise where students are required to use socio-technical feedback forms to reflect on their actual performance in crisis management exercises. Results from year 1 (N=83 participants), and year 2 (N=130 participants) indicate that this form of discussion exercise can function as a deeper learning artifact to help meet competence intended learning objectives (ILO) in information- and cyber security management courses. Results also suggest that experiential learning along with triple-loop learning will give the students a better platform to meet the increased need to consider alternative learning artifacts both to themselves and for learning in organizations in real life.

Keywords: Organizational learning, Information security, Crisis management.

## 1 INTRODUCTION

In the face of "profound change in organizational environments" [1], scholars have suggested that alternative forms of learning are necessary [1] to learn to apply complex problem solving skills to complex situations [2] like information- and cyber security incident response in socio-technical systems [3]. That is, we need to move from lectures and case-studies referred to as primarily and secondarily learning, to deeper learning like triple loop learning [1]. By using triple loop learning as an added learning form, the student should be able to consider what one has learned and how one can continue learning to make the most informed and hopefully optimal decisions.

In the Information Security MSc program at our university, an introductory course to management in information security is mandatory course in the program. Incident response is introduced in the literature [4], and a digital incident response discussion exercise have been introduced as a experiential learning artifact. The learning measurements (and thereby deliveries) in the discussion exercise have been a situational top-down brief (traditional), a BLUF, a management summary, and finally a draft for a press-brief, all being part of management communication in incident response. We have attempted to use such practical deliveries together with a socio-technical developed scenario for the purpose [5] to introduce triple-loop learning to the students through semi-structured discussions, for them to re-evaluate and consider the learning material over again.

In this paper we present the introduction and development of the discussion exercise in the introduction to information security management course over the last two years (course semesters of 2020 and 2021), together with feedback from the students, and results from learning measurements effects from a socio-technical survey executed amongst the students in the aftermath of the exercise, together with the actual performance from the deliveries.

After this introduction, the background of experiential learning and use of exercises are presented in section 2, before relevant crisis management foundations are presented in section 3. The method used to introduce the exercise is presented in section 4, before results and development are presented in section 5. Finally, conclusions and suggested future development are presented in section 6.

## 2 BACKGROUND

Experiential learning is often provided in courses to introduce the learner to the realities being studied [6]. The learning cycle in experimental learning "is a recursive circle or spiral as opposed to the linear, traditional information transmission model of learning used in most education where information is transferred from the teacher to the learner" [7].

The triple-loop-learning processing presented by Medema [29] can be described by three questions. The first question is “Are we doing things right?”. Likely to be an active experimentation based on theory, and then evaluate action and outcome of the experience. The second question is “Are we doing the right things?” which supports a dialogue about whether the rule of the game is ok, to think outside the box, and maybe be able to conceptualize changes. Finally, the question “How do we decide what is right?” should make the participants able to reflect upon what they learned in the process, and to be able to re-evaluate their own previous learning processes and whether it is beneficial to learn with other processes.

Discussion exercises can be described as “arranged situations wherein participants, under the guidance of a facilitator, interact in a scenario” [8] and as conceptual models in the terms of “abbreviated descriptions of reality” [9]. Discussion exercises can be used as deeper learning artifacts [10] to other learning materials in information- and cyber security management [11]. In addition, “discussion-based and conceptually oriented forms of crisis exercises are suitable for shaping an organization's crisis management capabilities by enhancing capacities relevant for the strategic and tactical aspects of crisis management” [8]. The authors suggest that by conceptualizing discussion exercises one would meet the socio-technical incident response challenges as a form of experiential and triple-loop learning. Thereby, the authors suggest that students will get better crisis management competence and be able to use their gained knowledge and skills in a real-life context.

The Homeland Security Exercise and Evaluation programs (HSEEP) has introduced a stair of training/exercises, where the next step of exercise includes elements of all the previous. Discussion exercises are not included as a step of its own but covers the four first steps of the stairs. The HSEEP approach is presented in figure 1.

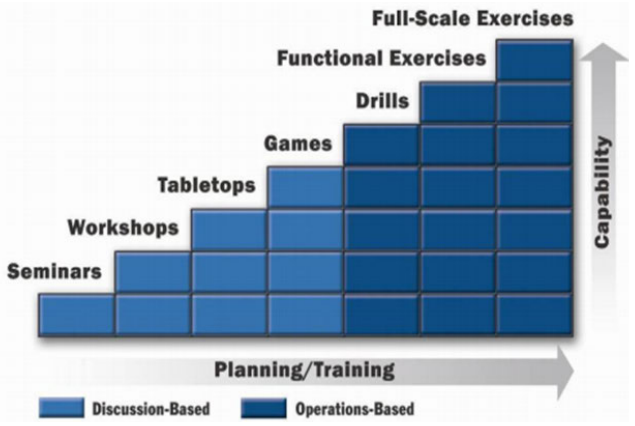



*Figure 1. Exercise Types and Capacity Levels [12]*

The Norwegian Directorate of Civil protection’s (DSB) method description of a discussion exercise [13] however, include elements from both seminars and workshops, but not necessarily table-top exercises, games, drills exercise etc.. In this paper, given that we are educating mostly Norwegian students, we have chosen the DSB method approach to better focus on the deeper learning artifact of a discussion exercise from a learning perspective [10].

To interact in a scenario for discussion exercises, root-cause analysis of previous incidents, and socio-technical analysis models, can be used to create relevant interaction-points [5], [14]. In addition, the scenarios should have a “semiotic framework to evolve the triple-loop learning technique from only handling the data, to further understand the necessity of information and thereby gain knowledge (and at some point, wisdom) of societal impacts” [15]. The FRISCO Semiotic Framework for IT communication [3, chap. 1] is suitable as a framework to create scenarios that include management considerations- and decisions [16], [17]. The introductory course being a large group of over 100 students, collective learning (in teams) was introduced through the Activity theory approach when developing the scenarios [18]. More specifically “to cover the subject, object and community, combined with activities, rules and division of labour”, better known as the basis for analysis in Activity theory [15], [18], [19].

Using a socio-technical backward design approach to prepare for the exercises [20], introductory lectures included, we suggest that the students also are given the possibility to "go back" and look at the lectures and literature after (and even during) the exercise. Comparable scenario-based exercises have been introduced by Grimaila [21] in an information security course at Texas A&M University.

## 3 THEORETICAL FOUNDATIONS

Traditionally crisis management theories have been centred around command- and control-systems (C2-systems) together with communication (emerging to C3-systems) where the "coordination normally occurs through the use of predetermined plans and procedures" [22]. One may, however, be in the situation where one needs to rely on the commander's intent instead of the plans, as anomalies may occur [22]. Directly transferable to Activity theory, one could say that you do the "activities" (actions), based on "rules" (plans and procedures) and "division of labour" (control-center), in the scenario covering "subject" (who does..), "object" (anomalies) and "community" (in this case where the military execution takes place).

Recent studies argue that also cognition is central to performance [23]. Cognition is defined as:

> *"the capacity to recognize the degree of emerging risk to which a com-munity is exposed and to act on that information" [23]*

Comfort [23] suggests that "without cognition, the other components (C3-systems) of emergency management remain static or disconnected". In addition, what would be referred to as distributed cognition, where

> *"the process of execution is described in terms of an information-processing activity, although what differentiates it from more standard accounts of human behaviour is that this information processing is not characterized in terms of individual cognition but as an emergent process arising from the coordinated actions of the team" [24], [25],*

leads us to introduce discussion exercises as a foundation to train together for information processing, leading to being prepared for coordinated actions in real life.

An essence in crisis management is the ability to make critical decisions in a turbulent environment [26].

> *"Critical decisions are an attempt to apply efficient modes of cognition and action to enable the organization to cope with consequential environmental threats or take advantage of important opportunities in the presence of highly restricted time in turbulent markets and/or specific situations." [26]*

Decision strategy systems [26] and decision support systems [27] have been suggested to support management in critical situations. In a discussion exercise during an introductory master course, we were afraid such support systems would "take away" the slow [28] and triple-loop-learning processing of these novices. Instead, they were provided with deliveries (initiated actions) to open for cognition.

## 4 METHODOLOGY

The authors addressed the competence shortage in the information- and cyber security management course by establishing a discussion exercise to learn incident management. We approached the challenge by using the design science research in information systems (DSRIS) [30]. Design science research (DSR) is a methodology which can be conducted when "creating innovations and ideas that define suggestions through the development process of artifacts which can be effectively and efficiently accomplished" [30]. In our case we proposed a learning artifact in the nature of a discussion exercise. How to work on DSRIS is presented in a thesis written by G. R. Karokola [31]. He visualized this approach as outlined in figure 2.

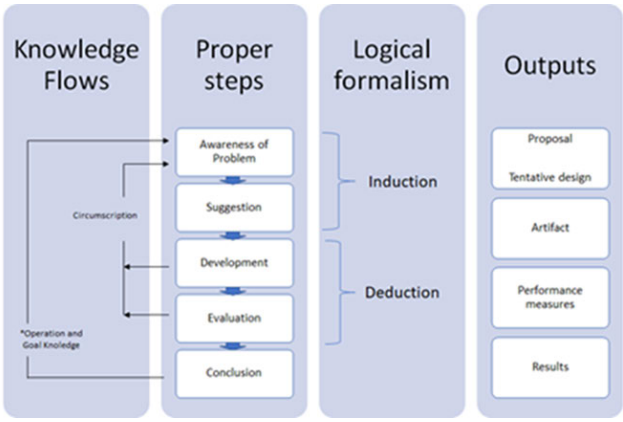



*Figure 2. DSRIS – modified from abduction to induction [31]*

However, logical formalism in figure 2 is in our research modified with an inductive approach instead of abductive approach used by Karokola. The inductivist approach starts by first observing a phenomenon and then generalizing about the phenomenon which leads to theories that can be falsified or validated [3].

Early on when we observed that the course was set up with a mandatory risk-analysis case, a term-paper project (research based) and an exam (multiple choice), we observed through extra-curricular activities with the students that managing incident-response challenges was too theoretical in the course. Experiences from working as crisis managers over years, makes the authors aware of how important managing crises are, and we suggested a discussion exercise for the course to meet the challenges (step 1 and 2 in the DSRIS).

To develop the exercise the modified socio-technical backward design model was used to outline the framework (step 3 in the DSRIS). The modified back-ward design model is presented in figure 3.

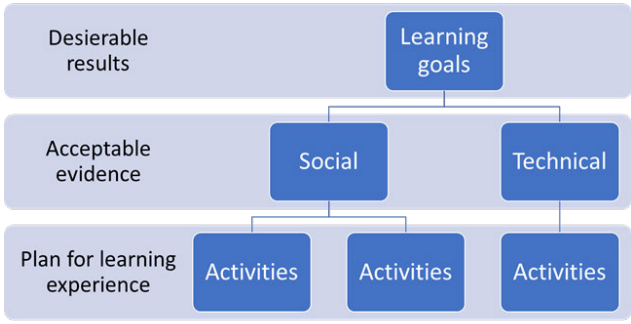



*Figure 3: Backward Design, modified in a socio-technical context [32], [20]*

The learning goals being socio-technical incident response management, both social- and technical "evidence" was introduced in the scenario covering introductory information about both cultural, structural, methods and machines in the scenario "community". The exercises had the same set-up, but the first exercise each year were executed with an insider scenario, while the second exercise each year were executed with an ATP-attack (advanced persistent threat attack) scenario (for the students in the second group to have the same surprise element as the first group), which can have had an impact on the results from the first and second exercise each year. These are therefore presented separately in this paper. However, scenario being the foundation for the discussion, and distributed cognition as the optimized way of managing the incident response, deliveries during the exercise (discussion) focused on a diversity of management communications and information, covering both top-down approaches, bottom-up approaches, reporting mechanisms as management summaries and finally creating a draft for a press-release on behalf of a top management group. A final activity was the lectures beforehand,

covering socio-technical incident response, but also giving examples of how to create the situational top-down brief, the BLUF, the management summary, and the press release.

The evaluations in the DSRIS-process were executed on both the lectures, the discussion exercise (as the learning artifact), the scenario (relevance), the student deliveries (performance deliveries) and thereby also the results.

## 5 ARTIFACT, FINDINGS, AND EVALUATION

Following the pathways of and outcomes of single-, double- and triple-loop learning [6], [29], [33], the discussion exercise had intended content of all types of loops. The content is presented in figure 4.

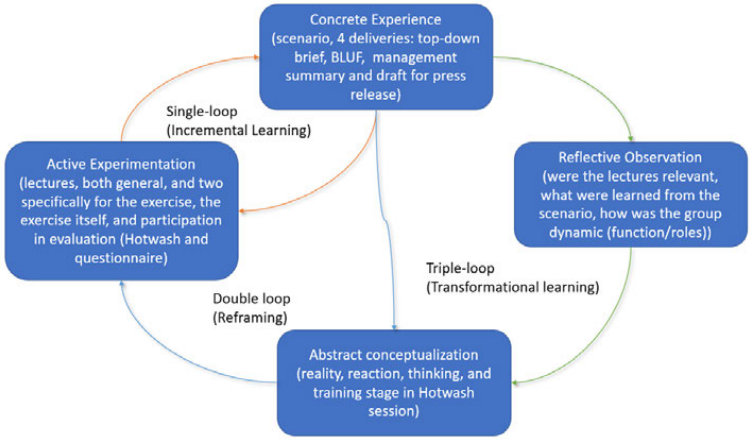



*Figure 4: Pathways of and outcomes of single-, double- and triple-loop learning adapted from Medema [29]*

The exercises were executed as a process, first presenting theoretical foundations and practical templates in lectures, before sending out the first stages of the scenario at lunchtime the day before the actual exercise. On the day of the actual exercise, the next stage of the scenario was introduced together with the first two deliveries at the beginning of the day, and later in the exercise the third stage of the scenario together with the last two deliveries were introduced. The deliveries had deadlines in the learning-system. After the last deliveries we had lunch, before the Hotwash session started. And, finally the individual student-evaluation (questionnaire) took place. All deliveries were reviewed, and feedback was given to all students on their performance.

Reports from the questionnaire were not distributed to the students, which could have added value to the reflective observation. As the questionnaire also were developed to meet the authors reflective observation, the current questionnaire requirement needs more alignment to the student's reflection goals.

### 5.1 Practical preparations

The students could choose between two different dates (university-regulations), and the dates were presented at the beginning of the semester. The groups were set up in the learning-system specifically for the exercise, and the assignments were also set up in the learning-system ahead of the exercise. The first year, the assignments had strict deadlines which led to some trouble with the deliveries. Thereby the deadlines in the system were extended a bit the next year, to make sure everyone would be able to deliver.

Student-assistants were responsible for registering all participants, and to do follow-up of questions regarding the learning-system throughout the exercise. Two alternative exercises were executed each year (mentioned university-requirements), mentioned in the following as 1) Year one, day one, 2) Year one, day two, 3) Year two, day one, and finally 4) Year two, day two.

We developed the questionnaire to reflect upon the learning goals, both from the lectures, the scenarios, and the deliveries. The following table 1 gives a summary of all participants and number of answers from the questionnaire.

*Table 1. Number of participants and number participating in the evaluation (questionnaire).*

| Exercise day | Number of participants = N | Number of answers = n |
|---|---|---|
| Year 1, day 1 | 70 | 51 |
| Year 1, day 2 | 13 | 11 |
| Year 2, day 1 | 120 | 77 |
| Year 2, day 2 | 10 | 8 |

The students were asked if they had participated in discussion exercises before, and what type of other exercises they might have participated in. Simulation exercises were explained to typically be red-team blue-team exercises. The results are presented in table 2 and table 3.

*Table 2. Previous experience from participating in discussion exercises.*

| | Participated in discussion exercise before. |
|---|---|
| **Year 1, day 1** | 35 (68,6% of n) |
| **Year 1, day 2** | 6 (54,5% of n) |
| **Year 2, day 1** | 52 (67,5% of n) |
| **Year 2, day 2** | 4 (50% of n) |

*Table 3. Other types of exercises they had participated in before.*

| | Table-top exercise | Full-scale exercise | Simulation exercise | Serious games |
|---|---|---|---|---|
| **Year 1, day 1** | 5 (9,8% of n) | 1 (2% of n) | 5 (9,8% of n) | |
| **Year 1, day 2** | 7 (63,6% of n) | 3 (27,3% of n) | 4 (36,4% of n) | |
| **Year 2, day 1** | 27 (35,1% of n) | 25 (32,5% of n) | 27 (35,1 of n) | 13 (16,9% of n) |
| **Year 2, day 2** | 5 (62,5% of n) | 4 (50% of n) | 3 (37,5% of n) | |

As we can see, a high number of the students had participated in exercises before (several students are part-time students or experience-based students), which could affect the group dynamics in the exercises. An added (not planned for) value to the reflective observation (either in the Hotwash session or in the questionnaire) could therefore be to evaluate what one can learn from such.

## 5.2 Lectures

In addition to the standard lectures based on the literature given in the course [4], two lectures were held to prepare the students for the exercise. One on crisis management and how to work in a crisis staff, and one on logs and information sharing. The students were asked how relevant they found the lectures beforehand to be. The results are presented in table 4.

*Table 4. Lectures relevance for the exercise*

| | No relevance | Some relevance | Relevant | Very relevant | Huge relevance |
|---|---|---|---|---|---|
| **Year 1, day 1 Crisis management** | 3,9% | 11,8% | 58,8% | 21,6% | 7,8% |
| **Year 1, day 1 Logs and information sharing** | 3,9% | 19,6% | 56,9% | 19,6% | 3,9% |
| **Year 1, day 2 Crisis management** | 0% | 9,1% | 27,3% | 54,5% | 18,2% |
| **Year 1, day 2 Logs and information sharing** | 0% | 27,3% | 54,5% | 27,3% | 0% |
| **Year 2, day 1 Crisis management** | 3,9% | 16,9% | 45,5% | 23,4% | 7,8% |
| **Year 2, day 1 Logs and information sharing** | 6,5% | 19,5% | 44,2% | 23,4% | 3,9% |
| **Year 2, day 2 Crisis management** | 0% | 0% | 75% | 25% | 0% |
| **Year 2, day 2 Logs and information sharing** | 0% | 12,5% | 62,5% | 25% | 0% |

A deeper focus on what would be the deliveries were presented in the lectures the 2nd year. That is, examples of the deliveries were posted in the learning system (in addition to the lectures themselves), which might be the reason for the better results on Very relevant in 2021.

## 5.3 Scenarios

The introductory scenario (sent out the day before the exercise) had a content of 1) exercise instructions with roles (to take on in the group) of an IT-management group at a big university, 2) background information in the form of a newspaper interview, 3) ICT-regulations at a university, 4) scenario introduction with a 5) local newspaper story. The next input (in the start of the exercise-day) had a content of 1) delivery instructions, 2) post on the wall from the security operation center (SOC), 3) content of a call (expectations) from the rector, 4) one local news-paper story, and 5) one national newspaper story. The final scenario-input had a content of 1) delivery instructions, 2) the "actual" situation, 3) one local newspaper story, and 4) one national newspaper story.

To validate if the scenario met the learning goals, questions about which of a variety of crisis tasks that can arise during an incident they felt they had achieved. The results are presented in figure 5.

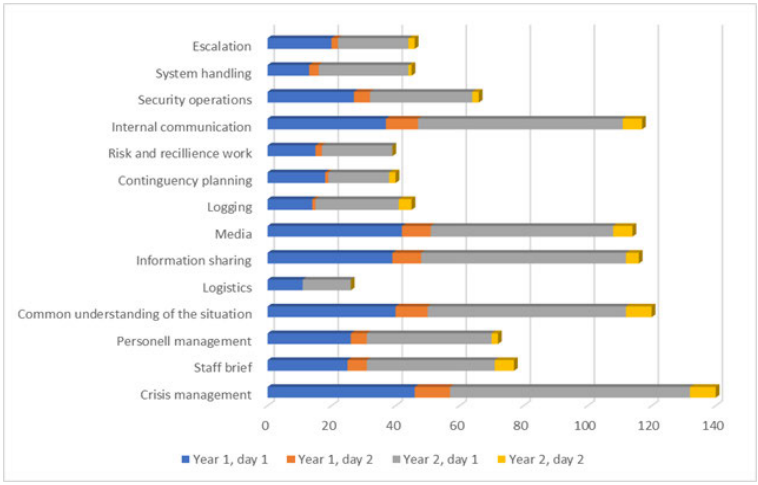



*Figure 5: Factors in the scenario the student scored as achieved.*

The five factors the students scored as mostly trained based on the scenario were, 1) internal communication, 2) media, 3) information sharing, and 4) crisis management. A small bias from these results would be that the deliveries also cover the three factors that scored with the highest results (supposed highest achievements).

## 5.4 Student deliveries

The results from the deliveries in the exercise varied in quality, but we could clearly see that those who had participated in the lecture beforehand managed better. One reason was e.g. that we explained what should be the content with examples in the templates in the lectures, so those who had participated changed it to be correct for the scenario presented in the exercise. Those who used the templates as is, hadn't really grasped all the content, but we gave explanations in the feedback they got. Two things were changed accordingly: Better stringent templates, and quicker feedback to the students.

## 5.5 Hotwash session

Studies have proven that Hotwash sessions can reduce stress in emergency services personnel [34] and have also shown positive effects in cyber-security exercises [35]. The discussion exercise being executed for a large number of students, a modified version of the Ebrahimian et. al Hotwash session [34] with two selected questions to meet the reality stage and the reaction stage for use in Mentimeter (everybody participating), and thereafter two selected questions to meet the thinking stage and training stage in a round-talk with all the groups (everyone listening in) were selected. The Mentimeter-questions are presented in table 5.

*Table 5. Reality and reaction stages in the Hotwash session.*

| | Use three words to describe what you think about the scenario? | Use three words to describe how you felt during the exercise? |
|---|---|---|
| Year 1, day 1 |  |  |
| Year 1, day 2 |  |  |
| Year 2, day 1 |  |  |
| Year 2, day 2 |  |  |

Unfortunately, when you move back and forward from one question to another in Mentimeter, you may answer the wrong question (both questions being prepared in the same shared folder), which you can see in some of the clouds. However, the bigger picture presented to the students was accurate enough, and the mission of the session was clearly met with open minds. The variety of thoughts about the scenario and feelings during the exercise, from relevant, interesting, and engaging on one side, to chaotic, simple, and boring on the other side, shows that the different student-groups did not necessarily have the same learning experience. Based on the variety of experience amongst the students as presented in table 1 and 2, this must also be expected in such an exercise. How to make the experienced-based students engage in how they can learn from the exercises and thereby not be "bored" could make the exercise even better in a triple loop learning context.

From the results of the next two questions (thinking stage and training stage) it also became clear that to take time to think about what you have participated in and what you have learned and will bring forward (and hopefully complete the triple-loop learning circle) was also of great importance. A few answers are selected from each question in every exercise, covering a variety of thoughts being presented.

*Table 6. Thinking stage and training stage in the Hotwash session.*

| | ***What was the most important thing you learned during the exercise?*** | ***What will you bring forward from the exercise?*** |
|---|---|---|
| ***Year 1, day 1*** | "Roles and responsibilities are important"<br>"Focus on the important information" | "Need to figure out how the incident-response plan should be" |
| ***Year 1, day 2*** | "Close to reality" | "Take the time to do good situational analysis" |
| ***Year 2, day 1*** | "Important to have an emergency plan"<br>"Who is responsible for what is important" | "Important to know what type of incidents that might occur" |
| ***Year 2, day 2*** | "Communication is essential"<br>"Importance of teamwork" | "You can only learn this through exercises" |

## 5.6 Student evaluation/questionnaire

It was important to us that the questionnaire would be a logical follow-up of the Hotwash session (from double-loop to triple-loop). In addition to already presented results, open questions were developed to obtain feedback from the students on what they thought could be improved in the exercise (for authors'

reflection as mentioned). After the first year's exercises, the most requested change, was to get a better understanding of what the different roles in the IT-management group were (functions in the roles). For 2021, we therefore wrote a paragraph per role presenting what their responsibilities typically are. Understanding the roles was also an issue the second year, but not to the same extent.

An unique feedback from one of the students the second year, was to present examples of state of the art deliveries (of the four) as a part of the Hotwash session, and that that would maybe give a better immediate learning experience. This will be considered for the 2022 semester. Another unique feedback suggested that time for reflections could have been done in between the interaction-points, not just at the end of the exercise. Timewise the exercise then will be extended, but the suggestion is relevant to meet the learning experience.

## 6 CONCLUSIONS AND FUTURE SUGGESTED DEVELOPMENT FOR THE EXERCISE

In this paper we have presented the introduction of a crisis management discussion exercise as an experiential incident response learning artifact to an information security management course at our university. Preliminary results suggest that experiential learning along with triple-loop learning adds values to the students learning experience and will be continued and developed in the course.

To develop and improve the artifact we will add one more reflection session, for the students to reflect on 1) teamwork/roles/functions, 2) learning from reports/results, and 3) extraordinary injections or deliveries to experienced students.

## ACKNOWLEDGEMENTS

It would not have been possible to execute the exercise without the student-assistants, and we will share our gratitude to the student-assistants positive energy and effort to make this possible.

## REFERENCES

[1] P. Tosey, M. Visser, and M. N. K. Saunders, "The origins and conceptualizations of 'triple-loop' learning: A critical review," *Manag. Learn.*, vol. 43, no. 3, pp. 291–307, 2012.

[2] J. Funke, "Complex problem solving: A case for complex cognition?," *Cogn. Process.*, vol. 11, no. 2, pp. 133–142, 2010.

[3] S. Kowalski, "IT Insecurity: A Multi-disiplinary Inquiry," Stockholm University, 1994.

[4] M. E. Whitman and H. J. Mattord, *Management of Information Security*. Cengage, 2018.

[5] G. ; Østby, L. ; Berg, M. ; Kianpour, B. ; Katt, and S. Kowalski, "A Socio-Technical Framework to Improve cyber security training: A Work in Progress," 2019.

[6] D. A. Kolb, "Experiential Learning: Experience as The Source of Learning and Development," *Prentice Hall, Inc.*, no. 1984, pp. 20–38, 1984.

[7] A. Kolb and D. Kolb, "Eight Important Things to Know About The Experiential Learning Cycle," *Aust. Educ. Lead.*, vol. 40, no. 3, pp. 8–14, 2018.

[8] J. Borell and K. Eriksson, "Learning effectiveness of discussion-based crisis management exercises," *Int. J. Disaster Risk Reduct.*, vol. 5, pp. 28–37, 2013.

[9] A. Adamsky and R. Westrum, "Requisite imagination. The fine art of anticipating what might go wrong," in *Handbook of cognitive task design*, E. Hollnagel, Ed. London: Taylor & Francis, 2003, pp. 193–220.

[10] K. S. Floyd, S. Harrington, and J. Santiago, "The Effect of Engagement and Perceived Course Value on Deep and Surface Learning Strategies," *Informing Sci. Int. J. an Emerg. Transdiscipl.*, vol. 12, pp. 181–190, 2009.

[11] S. A. Aderibigbe, "Can online discussions facilitate deep learning for students in General Education?," *Heliyon*, vol. 7, no. 3, p. e06414, 2021.

[12] HSEEP, "Homeland Security Exercise and Evaluation Program Volume 1: HSEEP Overview and Exercise Program Management," 2006.

[13] DSB, *Metodehefte diskusjonsøvelse*. 2016.

[14] P. Nyblom, G. Wangen, M. Kianpour, and G. Østby, “The root causes of compromised accounts at the university,” *ICISSP 2020 - Proc. 6th Int. Conf. Inf. Syst. Secur. Priv.*, no. July, pp. 540–551, 2020.

[15] G. Østby and S. J. Kowalski, “Introducing Serious Games as a Master Course in Information Security Management Programs: Moving Towards Socio-Technical Incident Response Learning,” in *Handbook of Research on Cross-Disciplinary Uses of Gamification in Organizations*, O. Bernades, V. Amorim, and A. Moreira, Eds. IGI Global, 2022, p. 24.

[16] L. F. H. Bento, R. O. Prates, and L. Chaimowicz, “Using semiotic inspection method to evaluate a Human-Robot Interface,” *2009 Lat. Am. Web Congr. - Jt. LA-WEB/CLIHC Conf.*, pp. 77–84, 2009.

[17] K. C. Desouza and T. Hensgen, “Semiotic emergent framework to address the reality of cyberterrorism,” *Technol. Forecast. Soc. Change*, vol. 70, no. 4, pp. 385–396, 2003.

[18] M. Gross and S. M. Ho, “Collective Learning for Developing Cyber Defense Consciousness: An Activity System Analysis,” *J. Inf. Syst. Educ.*, vol. 32, no. 1, pp. 65–77, 2021.

[19] Y. Engeström, *Learning by expanding - An activity theoretical approach to developmental research*, 2nd ed. UK: Cambridge University Press, 2019.

[20] G. Østby and S. J. Kowalski, “Preparing for Cyber Crisis Management Exercises,” in *n: Schmorrow D., Fidopiastis C. (eds) Augmented Cognition. Human Cognition and Behavior. HCII 2020. Lecture Notes in Computer Science, vol 12197.*, 2020, pp. 279–290.

[21] M. R. Grimaila, “A novel scenario-based information security management exercise,” *2004 Inf. Secur. Curric. Dev. Conf. InfoSecCD 2004*, pp. 66–70, 2004.

[22] L. G. Shattuck and D. D. Woods, “Communication of Intent in Military Command and Control Systems,” *Hum. Command*, pp. 279–291, 2000.

[23] L. K. Comfort, “Crisis management in hindsight: Cognition, communication, coordination, and control,” *Public Adm. Rev.*, vol. 67, no. SUPPL. 1, pp. 189–197, 2007.

[24] M. Perry, *Distributed Cognition*, no. December 2003. 2018.

[25] E. Hutchins, “Cognition in the wild,” in *Cultural cognition*, London: The MIT Press, 1995, pp. 352–374.

[26] M. Coccia, “CRITICAL DECISIONS IN CRISIS MANAGEMENT: RATIONAL STRATEGIES OF DECISION MAKING,” *J. Econ. Libr.*, vol. 7, no. 2, pp. 81–96, 2020.

[27] O. Kulikova, R. Heil, J. Van Den Berg, and W. Pieters, “Cyber crisis management: A decision-support framework for disclosing security incident information,” in *Proceedings of the 2012 ASE International Conference on Cyber Security, CyberSecurity 2012*, 2013, pp. 103–112.

[28] Simon, “Simon 1987.pdf.” .

[29] W. Medema, A. E. J. Wals, and J. F. Adamowski, “Multi-Loop Social Learning for Sustainable Land and Water Governance : Towards a Research Agenda on the Potential of Virtual Learning Platforms,” no. July 2018, 2014.

[30] W. Kuechler and V. Vaishnavi, “A Framework for Theory Development in Design Science Research: Multiple Perspectives,” 2012.

[31] G. R. Karokola, “A framework for Securing a-Government Services, The case of Tanzania,” Stockholm University, 2012.

[32] G. Wiggins, G. P. Wiggins, and J. McTighe, *Understanding by Design*. ASCD, 2005.

[33] C. Folke, T. Hahn, P. Olsson, and J. Norberg, “A DAPTIVE G OVERNANCE OF S OCIAL-ECOLOGICAL SYSTEMS,” 2005.

[34] A. Ebrahimian, S.-M. Esmaeili, A. Seidabadi, and A. Fakhr-Movahedi, “The Effect of Psychological Hotwash on Resilience of Emergency Medical Services Personnel,” *Emerg. Med. Int.*, vol. 2021, pp. 1–7, 2021.

[35] J. Vykopal, R. Ošlejšek, K. Burská, and K. Zákopčanová, “Timely feedback in unstructured cybersecurity exercises,” *SIGCSE 2018 - Proc. 49th ACM Tech. Symp. Comput. Sci. Educ.*, vol. 2018-Janua, pp. 173–178, 2018.

Publication 4

Østby, Grethe; Katt, Basel. (2019) Cyber Crisis Management Roles – A Municipality Responsibility Case Study. *Information Technology in Disaster Risk Reduction.* Springer.

# Cyber Crisis Management Roles – a Municipality Responsibility Case Study

Grethe Østby and Basel Katt

Norwegian University of Science and Technology, Gjøvik, Norway
{grethe.ostby;basel.katt}@ntnu.no

**Abstract.** In this paper we propose a role model that can be applied in societal cyber crisis management to build safety and standard procedures during cyber security crisis. We define societal cyber crisis as the cyber crisis which affect the society in which disaster is or might be the consequence. The process to create our model started by analyzing regulations and responsibilities in Norwegian municipalities, and we used steps of a design science research (DSR) research approach to create our suggested artifact. A combination of conventional crisis management and cyber crisis management is proposed to identify the interrelationships among diverse stakeholders when managing the preparation for and reaction to a cyber crisis incident. We present a cyber incident handling role model (CIHRM) which is usable for visualizing cyber crisis in a diversity of organizations. After our model has been reviewed by the cyber security research community, we plan to implement the model when analyzing crisis management in various organizations to prepare for instructions, training and exercises at our training environment - The Norwegian Cyber Range.

**Keywords:** Cyber crisis, Cyber management, Management roles, Crisis management, Societal cyber crisis.

## 1 Introduction

Bruer research has shown that the current competence levels on digitalization process among leaders in public sector in Norway has led computer security activities to be isolated from strategic planning daily operation [1]. Consequently, upper management leaders is focused on efficiency, rather than society readiness and emergency preparedness [2]. This is also supported by the Norwegian Auditor General's administration study nb 1, 2018 about digitalization in governmental sector, which concluded that the digitalization among departments and directorates is going too slow [3]. Cyber security and safety are not mentioned in any part of the report, only personal information in the matter of how to transfer these data from one department to another, and consequently the managers are forced to focus on the digitalization.

However, NOU 2015: 13 Digital vulnerability – safe society (Lysne committee), is describing how the civil protection system also should include the handling of cyber-incidents, both system failures and malicious attacks [4]. At the same time the Lysne committee also observed that there is lack of a cyber-security arena within the sector of

the municipalities. They described that many municipalities have an increased need of counselling and education to make good risk- and resilience analyses, and to establish control-systems to handle cyber-incidents. In addition, a municipality CERT is recommended in the study of municipalities common need of competence-center to deal with handling cyber-security incidents made by NorSIS 2017 [5].

In general, between an individual and an organization, there are teams, and more specifically, crisis management groups. Groups of people and teams from different worlds, with very different cultural responses to risk and emergency, having often very distinct prejudices about the threats to be dealt with and the goals to be met, and whose individual and corporate interests lend themselves poorly to broader cooperation. And they are all expected to work together under pressure [6].

In Norwegian (and other countries) traditional emergency-organizations, as for example the military forces, the police forces, the civil defense forces and others, roles have been defined to avoid dependency on individuals and to have a long-time rollover in these roles. Norwegian governmental regulations and guidance on municipalities' responsibilities is still suggesting tasks to be managed, and crises to be led by the municipality management. For several years, roles in such crisis responsibilities have been suggested in a number of municipality crisis management courses run by the Norwegian Civil defense national competence center, which those municipalities have adopted and have used with success during crisis.

The Norwegian municipality guidance suggests establishing a crisis staff to sup-port the crisis management, but it does not define the roles of the staff. A lot of tasks are outlined, but they are not regulated in roles to deal with them [7]. Thus, it is easy to understand why decision makers responsible for crisis management want ways to respond to these challenges. It is important to recruit competent individuals, but it is also crucial to build teams and organizations that compensate for moments of individual weakness [6]. In this paper, we try to tackle these issues by studying two com-parable crises with different causes. These crises could be analyzed within organizational tiers and thereby model roles and tasks to handle a variety of crisis, specifically societal cyber crisis. We use the municipality crisis management responsibility as a case to combine this responsibility with cyber crisis which affects municipality society. We aim to combine traditional incident command system roles with the organization–governed networks responsibilities.

Based on the analyzed crises, we suggest a model to best implement roles in management teams of societal cyber crisis on how to handle the crisis. We define societal cyber crisis as cyber crisis which affect the society in such a context of which disaster is or might be the consequence. We discuss the cyber incident management in all phases of the crisis on strategic, tactical and operational tiers in organizations to sup-port other/overall crisis management decisions. Cyber-incidents require vast knowledge on all tires, and there will be a need of bringing in diverse experts in management-teams on the different tires, such as experts from SOCs, CERTs and other real-life stakeholders. These vast tasks require excellent capabilities to manage such teams and will be one of the most important ranges of roles to frame for managing societal cyber crisis.

The paper is structured as follows: After the introduction in section 1, in section 2 the background and relevant literature is presented. In section 3, our research approach

is discussed together with the use of municipalities crisis management responsibilities. In section 4, we present the municipality management roles, and discuss how to bring in cyber crisis roles. In section 6 we exemplify the outcome of our model and outline our prospects for further research.

## 2 Background and relevant literature

In the literature on social–ecological systems, the term 'resilience' is used to de-scribe the ability of a system to absorb or withstand changes inflicted onto the system from the outside [8]. Walker et al. [8] define the resilience of a system as: the capacity of a system to absorb disturbance and reorganize while undergoing change to still retain essentially the same function, structure, identity, and feedbacks. Resilience research is also interested in studying what kind of interactions can occur in complex interdependent infrastructures, but not with the aim to only identify the most critical relations. Rather, the aim is that operators and middle managers learn about complex system behavior to enable them to perform real-time resilience, or "operating at the edge of failure without falling off" [9]. Risk analysis, business continuity management and crisis management training are often performed within the context of a single organization or sector and are seldom addressing the holistic analysis of multiple infrastructures [9].

The process of disaster management is commonly visualized in several phases. The disaster management cycle illustrates the ongoing process by which governments, businesses and civil society plan for and reduce the impact of disasters, react during and immediately following a disaster, and take steps to recover after a disaster has occurred. The significance of this concept is its ability to promote a holistic approach to disaster management as well as to demonstrate the relationship between disasters and development. The pre-disaster activities are done before the hazard interacts with the vulnerable community to cause a disaster, usually referred to as mitigation and preparedness, which includes major activities such as preparedness through response, from prevention, mitigation and readiness, through relief, recovery and rehabilitation [10].

Disaster management is dealing with the immediate aftermath of the disaster, including short-term relief and response. This relates to activities such as evacuation, search and rescue and medical care. Post-disaster is the period of recovery until community returns to a normal condition. The concept of sustainable development is frequently associated with long-term recovery, which strongly aligns to the multiple-state definition of resilience, whereby a community should maximize the capacity to adapt and focus on long-term growth to a state of reduced vulnerability [11].

The NIST Framework for Improving Critical Infrastructure Cybersecurity, commonly referred to as the NIST Cybersecurity Framework, provides organizations with a structure for assessing and improving their ability to prevent, detect and respond to cyber incidents. Version 1.0 was published by the US National Institute of Standards and Technology (NIST) in 2014 and was aimed at operators of critical infrastructure. The framework guides cybersecurity activities and considers cybersecurity as a part of an organization's risk management processes. In this paper we present a model for the response and recovery phase as suggested in figure 1.


**Fig. 1.** NIST Cyber security framework [12]

From a cyber security incident perspective Kulikova et. al. [13] suggests four steps in crisis management comparable to NIST's framework, and FEMA suggests four stage activity cycle of mitigation, preparedness, response and recovery [15]. These approaches are comparable to NIST, and response and recovery are important in all suggestions.

As mentioned before, there should be roles pre-defined to cope with the response and recovery. When an emergency is unfolding, the people and systems involved in watching it unfold must determine what has already happened, what is currently happening, and what is likely to happen in the future; then, they make recommendations for reaction based on their situational awareness [15]. To be able to understand the situation, the responsible staff role should be able to visualize the incident.

As van der Aalst pointed out, event data is the major source of information [16]. Therefore, all these available events are numerous and the data and information they contain is more or less reliable, comes from varied sources, in various types and formats, and are time-dated. Incident Command Systems (ICS) is used to coordinate multiple response organizations under a temporary central authority with a hierarchical structure [17]. It is better understood as a highly centralized mode of network governance, designed to coordinate interdependent responders under urgent conditions. The contrast between a network governance and hierarchical view of the ICS is illustrated in figure 2. The left-hand side of the figure represents the dominant view of the ICS [18]. In this figure, a hierarchy allows the incident commander to direct the crisis functions of logistics, operations, planning, and finance/administration. But if we consider the ICS in terms of its members, we see it as a network, albeit a highly centralized one (on the right-hand side). The incident commander is at the center of the network, surrounded by organizations that have ongoing inter-crisis dyadic relationships, as illustrated by the right-hand side of figure 2.

When it comes to roles, the National Institute of Standards and Technology (NIST) has ranged three different tiers in the framework of risk management, which can help organize roles in these tiers. These tiers are strategic, tactical and operational [19] (figure 3).

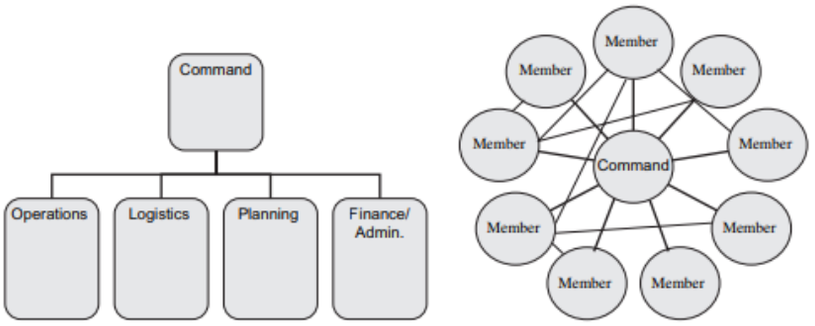



**Fig. 2.** Traditional incident command system and organization–governed networks [17]


**Fig. 3.** Tiers in framework of risk management (NIST)

Every tier is led by managers, and different crises require different management roles on each layer. This can be transferred into diverse organizations on national, sectorial and local public responsibilities.

Boeke investigates how different models of public–private partnerships shape cyber crisis management in four European countries: the Netherlands, Denmark, Estonia, and the Czech Republic. Using Provanand Kenis's modes of network governance, an initial taxonomy of cyber governance structures, he presents two suggestions: First, national CERT/CSIRT teams are to be embedded inside or outside the intelligence community. Second, if cyber capacity can be centralized in one unit or spread across different sectors [20].

In this paper, we use the municipality crisis management responsibility as a case to discuss cyber crisis which affects municipality society to argue for a solution which combine Boeke's suggestions. We aim to combine traditional incident command system roles with the organization–governed networks responsibilities as outlined in this section.

## 3 Research approach

In this paper, we approach the cyber security challenges using what can be referred to as a naive inductivist approach. The naïve inductivist approach starts by first observing a phenomenon and then generalizing the phenomenon which leads to theories that can be falsified or validated [21]. This approach will use the methodology out-lined by design science research in information systems (DSRIS) [22]. This methodology uses artifact design and construction (learning through building) to generate new knowledge and insights into a class of problems.

DSRIS requires three general activities: (1) construction of an artifact where construction is informed either by practice-based insight or theory, (2) the gathering of data on the functional performance of the artifact (i.e., evaluation), and (3) reflection on the construction process and on the implications the gathered data (from activity (2)) have for the artifact informing insight(s) or theory(s) [22].

How to work on these steps was presented in a thesis written by Karokola [23]. He visualized this approach as outlined in figure 4. As we are approaching our work in a naive inductivist approach, we modified the logical formalism in the model from abduction to induction.

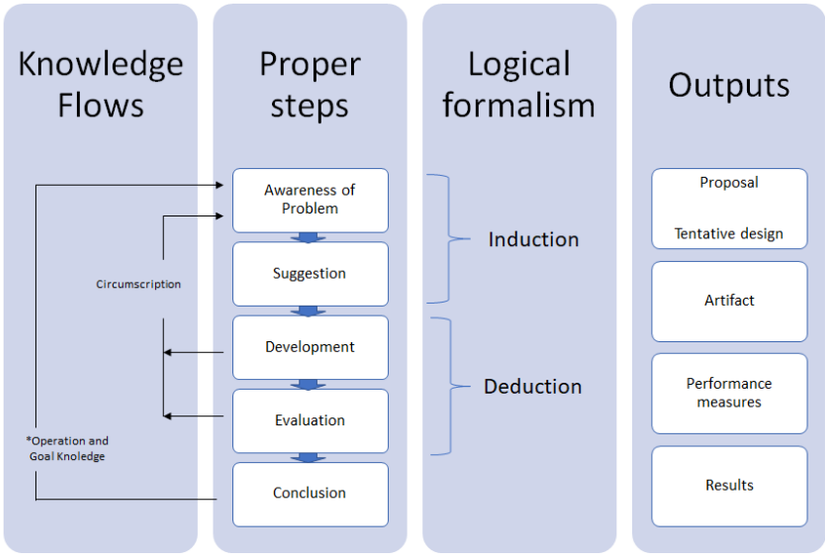



**Fig. 4.** Design research methodology - modified

To propose an artifact in an inductive approach we started up by analyzing municipalities responsibilities when handling crisis in general and cyber-incidents in special (first step in the 2nd column). For the next step we suggest a model to deal with the problem in crisis management when handling cyber incidents (second step in the 2nd column). The goal of the paper is to propose a tentative design (first step in the 4th

column), in which we want to present and test when executing cyber training and exercises in our training environment.

**Apply the case of municipalities crises management responsibilities**

The Norwegian law concerning the municipality's emergency duty, civilian preparedness and the Civil defense organization outlines the municipality's responsibility to analyze and make emergency preparation based on risk and resilience in their geographical designated area [24].

The municipalities should outline prepared societal emergency work that will [25]:

- Protect the population and contribute to uphold critical infrastructure.
- Give an overview of knowledge and awareness of societal critical challenges and what effect these challenges would have on the society and communities.
- Reduce risk and vulnerability through preventive work.
- Ensure good emergency preparedness and crisis contingency.
- Attend to ensure collaboration and coordination with internal and external societal emergency partners in the municipality.

In this idea-paper, we start by presenting as-is crisis-management roles that are defined and evolved based on the guidelines and try to combine this with roles needed in a cyber crisis.

# 4 Cyber incident handling role model – a municipality case study

In this chapter we propose a cyber incident handling model to best implement roles in management teams of societal cyber crisis on how to handle the crisis. We discuss the cyber incident management in the respond and recovery process of the crisis on strategic, tactical and operational tiers in a municipality case. We suggest bringing in diverse experts in management-teams on the different tires, such as experts from SOCs, CIRTS and other real-life stakeholders. We present the as-is responsibilities in the municipality's regulations and guidance on crisis management as introduction to our arguments and the modelling and give a summary of the roles in the end.

## 4.1 Municipality regulations and guidance

DSB's guidance recommends that the roles and responsibilities should be described in the contingency plan, the municipalities crisis management is to be understood as a critical societal function, and is supposed to be maintained throughout any event, no matter of time, both in peace, security political crises and in armed conflicts. The guidance also suggests that the municipalities crisis management can be expanded by supporting personnel and subject responsibilities, dependent on the crisis nature and extent.

Our experience in this matter is that it takes too much effort not to start out with the necessary experts to begin with, and that it is better to call out subject responsibilities

which will adapt to the incident, and then dismiss staff as the crisis is going into pre-crisis phase. We suggest key personnel to be on predefined roles-lists, to quickly do replacement in the specific subject role.

The guidance suggests that the municipality should consider the need of safety-clearance of key personnel in the crisis management. To be able to consider who needs this clearance, roles must be defined, and what personnel can fill the roles. This also supports our suggested role-modelling.

The guidance suggests the crisis management to be prepared on the following:

- Quickly decide efforts within the municipality's responsibilities, i.e. public information establishes evacuation center and psycho-social support teams.
- Be the public "face" and ensure good communication with the population, inter-nal employees and media.
- Attend to coordinate local handling of the crisis through internal and external societal security organizations.
- Provide recourses to handle crises based on contractual agreements.
- In special cases – discuss priorities and diffusion of limited recourses in collaboration with other societal critical organizations, and neighboring municipalities.
- Communicate needs of resources to the county or/and other regional security organizations.
- Surveillance of the situation, and dialogue with other emergency organizations affected by the crisis.
- Develop and communicate gathered understanding of the situation based on information from the responsible department in the municipality.
- Inform the political parties on a regular timeline
- Inform county on collaboration channel
- Make sure substitute/deputy personnel is in place in case of regular members absence.

The guidance suggests establishing a crisis staff to support the crisis management, but it does not define the roles of the staff. As you can see a lot of tasks is outlined, but they are not regulated in roles to deal with them. We suggest the diversity of crisis responsibilities roles should be defined on strategic level, tactical level and operational level.

### 4.2 Different crises, comparable roles

Typically, the strategic level consists of the municipality's management, the tacti-cal levels consists of the managers running the different local municipality elderly homes, schools, kindergartens, water-supply departments etc., while the operational level consists of staff and employees on the ground, like doctors, nurses', teachers and engineers. When the incident is an elderly home on fire, the roles in the organiza-tion based on regular crisis, and crisis management regulated in contingency plans. When the incident is an elderly care-taker system out of order, the need of ICT-expert teams is necessary, and regular crisis management roles does not cover experts need-ed. There is a need to

include these roles, as regular municipality crisis management might not have the competence to handle those crises. However, the crisis still must be handled manually by the regular crisis management. This means that a cyber crisis will need additional management and will thereby be more challenging to handle. Our discussion is visualized in figure 5.

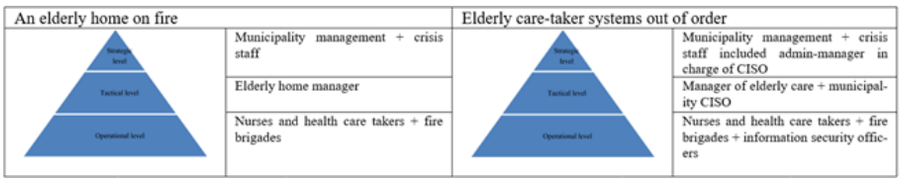



**Fig. 5.** Regular crises vs. cyber security crises

As suggested in the guidance it is the municipality management with their responsibilities which should take the roles as crisis management. In a crisis as suggested – fire at the elderly home, some managers will be more affected than others, and it is of course the health and elderly manager that will follow up on the employees, elderlies and their situation. The chief municipal executive will take the role as the crisis manager and will make sure that other members of the crisis management less influenced by the incident contribute with necessary supply and logistics. The major will follow up on media information, meet the elderlies and their next of kin. To get necessary support on media tasks, the major typically get support from a press coordinator. In such a crisis both the police contact, a fire brigade officer and the chief municipal medical officer will be a part of the crisis management to bring situational awareness into the group. They will get updates from forces alarm centrals and the forces alarm centrals get update from operative teams at the elderly home.

Crisis management and/or staff management is set up as a team working together in a safe environment to ensure the contingency of the management throughout the crisis. The regulations require a plan to move the crisis management if necessary [26]. The crisis management is therefore in need of the right information about the situation to make the right decisions. On the other hand, the information needs outside the crisis management is also not just pushing boundaries to the regular organization but are vast and mixed as visualized in figure 6.

These information needs require extra focus and handling during crises, and we have chosen to define information roles as requested in the regulations, as separate roles in the crisis management [26]. These roles are also specifically outlined in figure 7, on both strategic, tactical and operational levels.

On the tactical level the health and elderly manager team will support the elderly home manager with regulations from the contingency plans, more specific evacuation and necessary health support from next door municipalities etc. On operational level the elderly home manager will follow up on drilled tasks in such an incident.

As mentioned before, information in such crises is vital, and the tactical information team will monitor information in the crisis management systems, in newspapers and social media. They will also publish information both external in social media, and

internal to the employees in the municipality. And of most importance: support and gather information back and forth to the 1st line service desk personnel. 1st line service desk personnel are commonly strengthened with more personnel in such crises. This regulated way of handling crisis is presented in figure 7.

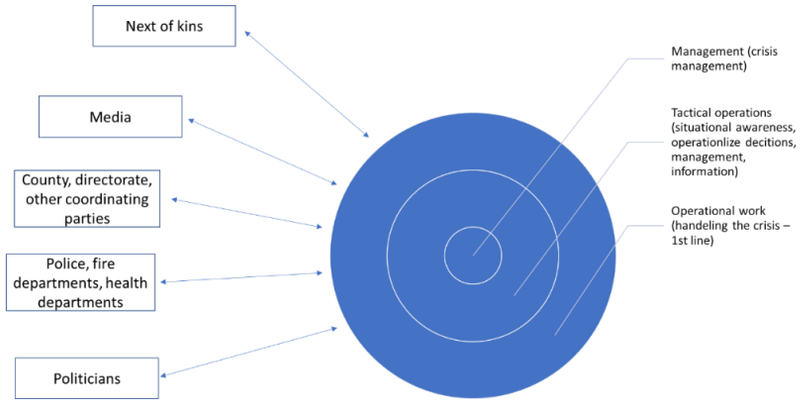



**Fig. 6.** Needs of crisis information

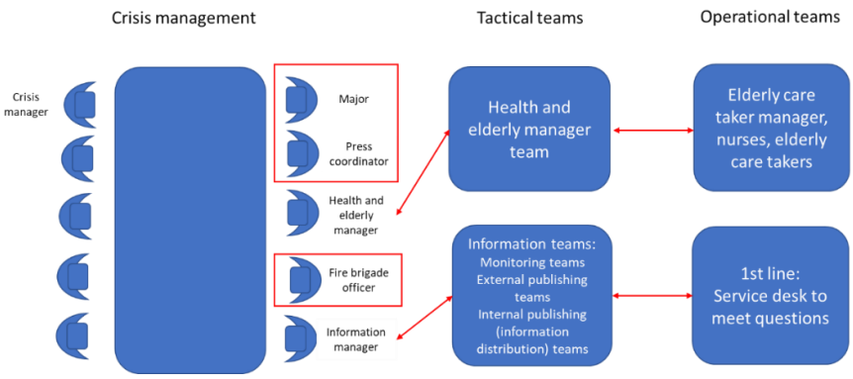



**Fig. 7.** Incident handling roles in conventional crises management

As previously stated regarding our other suggested crises: an elderly care-taker system out of order, that will require additional tasks. We have discussed which other roles could have incorporated these tasks, but as the principle of nearness and likeness is the foundation of crisis management, we suggest new roles to support the crisis.

First, we suggest that the municipality ICT-manager should be a part of the crisis management. In such a case the timeline to provide redundant systems or get the system back up and running is crucial information to the crisis management decisions. Next a tactical ICT management team should coordinate information between the management and the operational teams and get the responsibility to communicate with municipality

CERT and organizations like National security authorities if necessary. Third, at operational level, investigation and recovery operations like suggested by NIST cyber security framework (figure 1) should take place.

Additionally, the operational cyber team should collaborate with police investigators and system users. The other tasks during the crisis remain the same as in any other crisis. Our suggested additional roles during cyber incident crisis is visualized in figure 8.

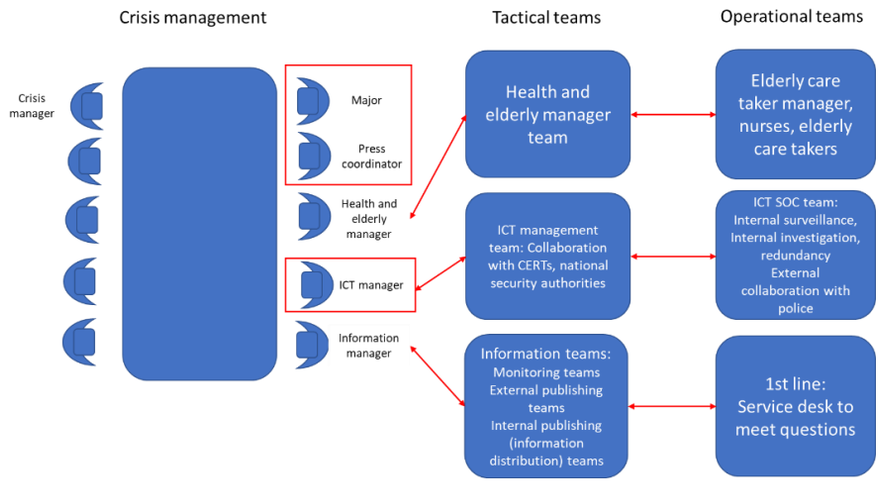



**Fig. 8.** Incident handling roles in cyber security crisis

As the mentioned digitalization is increasing, one may also argue the necessity of this type of organization in any societal crisis. To exemplify this, we argue the need of ICT personnel in the mentioned fire at the elderly home were an evacuation will take place, but also in conventional crises like forest fires, floods, hurricanes and others.

All information flow in such crisis is today digitalized, and to follow up information security and prepare for redundant information flow during any crisis, we suggest the ICT-roles as an essential part of the crisis management on a regular basis, regulated in contingency plans.

### 4.3 Summary

Using well known crises to visualize and implement cyber crises in municipality crises management appear useful in understanding and defining roles as it gives us a good indication about relevant tasks and information sharing on both strategic, tactical and operational level.

An overview of municipality crisis management roles when cyber crisis occur is presented in table 1.

**Table 1.** Tasks and roles in societal cyber crises: an overview

| | Management roles | Internal team tasks | External team tasks |
|---|---|---|---|
| Strategic | Chief municipal executive<br>Municipality management<br>Major<br>Press coordinator<br>Information manager<br>ICT-manager: | Chief municipal executive leading the crisis<br>Municipality management = crisis management handling crisis in departments<br>Major and press coordinator meet media, elderlies and next of kin<br>Information manager coordinates all information<br>ICT-manager:<br>Managing ICT-crisis | Might be coordinated by county governor and directorate |
| Tactical | Department manager team<br>Information teams<br>ICT management team | Health and elderly manager team:<br>Follow up on the employees, elderlies and their situation<br>Information teams:<br>Monitoring teams<br>External publishing teams<br>Internal publishing (information distribution) teams<br>ICT management team:<br>Collaboration with CERTs, national security authorities | Other municipalities<br>CERT<br>NSM |
| Operational | Operational manager and employees<br>ICT SOC Team<br>Municipality service desk | Elderly care-taker manager, nurses, elderly care takers:<br>ICT SOC team: Internal surveillance,<br>Internal investigation, redundancy<br>External collaboration with police<br>1st line:<br>Service desk to meet public questions | Police investigators |

## 5 Conclusion and future research

The cyber incident handling roles model (CIHRM) presented in figure 8 is usable to visualize both regular crisis and cyber crisis. We propose to name this crisis handling visualizing model a cyber incident handling role model (CIHMR).

Visualizing crisis tasks and roles enables us to introduce more holistic and near-to-life elements needed to be factored in handling crisis. We need to verify and validate the findings suggestions we have made, and to enhance and improve the cyber inci-dent management roles in more detail. To validate the framework, we plan to test suggested roles model when setting up exercises in our training environment, the Nor-wegian Cyber Range (NCR). NCR will be an arena where testing, training, and exer-cise are tools to expose people, businesses, and units to realistic events and situations in a realistic but safe environment. The arena ensures efficient transfer of knowledge and building of real-world competence, that links together the strategic, operational, tactical and technical levels of decision making, by simulating the impacts of cyber security events on the levels of society, digital value chains and cyber infrastructure without harming the entities involved and their critical infrastructure.

In this paper we propose roles by using only one specific example of cyber crisis. In future work we will test if these roles are transferable to other societal emergency cyber crises. We intend to use the cyber incident handling role model (CIHRM) pre-sented in figure 8 to visualize cyber crisis in various aspects of cyber crisis.

To ensure the best possible effect in the NCR, current suggested roles and tasks will be facilitated as most accurate comprehension of exercises fitted the different roles. Additionally, there will be need of preparedness learning based on real life incidents. We plan the preparedness learning as instruction for adults using action research by instructors with reflection throughout lectures.

When analyzing the outlined definitions of roles, we found that there is no clear definition of cyber crisis management roles. We based the suggested roles on NIST management tiers and will also need to consider NATO management tiers. Moreover, as mentioned before, there are examples of real-life incidents roles which might be analyzed to compare best practices. We consider this as an area, which can be devel-oped better in combining role-definitions and scenarios and have a long-time work in progress in this matter.

## References


1. Bruer, A.: Ny undersøkelse: Stort etterslep på mellomlederes IT-kompetanse i offentlig sector. digi.no, 09-Aug-2017.
2. Baugerød Stokke, O. P.: Advarer it-sjefer mot effektivitet. Computerworld.no, 23-Mar-2009.
3. Office of the Auditor General of Norway, “admin report nb. 1, (2018).
4. NOU 13 Lysne commitee, “Digital vulnerability – safe society,” (2015).
5. NorSIS: The study of municipalities common need of competence-center to deal with handling ICT-security incidents, (2017).
6. Lagadec, P.: PREVENTING CHAOS IN A CRISIS Strategies for prevention, control and damage limitation Preface : tools for thinking about, preventing, and managing crisis ix. (1993).
7. DSB: Municipality guidance, emergency duty. (2017).
8. Walker, B. Holling, C. S. Carpenter, S. R. and Kinzig, A.: Resilience, Adaptability and Transformability in Social–ecological Systems. Ecol. Soc., (2004).

9. De Bruijne, M. and Van Eeten, M.: Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment. (2007).
10. De Guzman, E. M.: Towards Total Disaster Risk Management Approach. (2002).
11. Haigh, R. and Amaratunga, D.: An integrative review of the built environment discipline's role in the development of society's resilience to disasters. International Journal of Disaster Resilience in the Built Environment, 1(1), pp. 11–24, 26-Feb-2010.
12. Anderson, E.: How to Comly with the 5 Functions of the NIST Cybersecurity Framework. Forecoun, (2017). [Online]. Available: https://www.secmatters.com/blog/how-to-comply-with-the-5-functions-of-the-nist-cybersecurity-framework.
13. Kulikova, O. Heil, R. Van Den Berg, J. and Pieters, W.: Cyber crisis management: A decision-support framework for disclosing security incident information. in Proceedings of the 2012 ASE International Conference on Cyber Security, CyberSecurity 2012, pp. 103–112 (2013).
14. FEMA: The Federal Emergency Management Agency Publication 1. (2016).
15. S. L. Pfleeger and D. D. Caputo: Leveraging behavioral science to mitigate cyber security risk. Comput. Secur., (2012).
16. van der Aalst, W. M. P.: Data Scientist: The Engineer of the Future. (2014).
17. Moynihan, D. P.: The network governance of crisis response: Case studies of incident command systems. Journal of Public Administration Research and Theory, 19(4), pp. 895–915, (2009).
18. Fema: National Incident Management System. (2017).
19. Locke G. and Gallagher, P. D.: Managing Information Security Risk Organization, Mission, and Information System View Joint Task Force Transformation Initiative Nist Special Publication 800-39, (2011).
20. Boeke, S.: National cyber crisis management: Different European approaches. Governance, vol. 31, no. 3, pp. 449–464, (2018).
21. Kowalski, S.: IT Insecurity: A Multi-disiplinary Inquiry: Stockholm University. 1994.
22. Kuechler, W. and Vaishnavi, V.: A Framework for Theory Development in Design Science Research: Multiple Perspectives. (2012).
23. Karokola, G. R.: A framework for Securing a-Government Services, The case of Tanzania: Stockholm University, (2012).
24. Justis- og beredskapsdepartementet, "Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (sivilbeskyttelsesloven)." Norwegian Government, (2010).
25. DSB, Guidance to holistic risk and vulnerability assessment in the municipality. DSB, (2019).
26. Norwegian government, FOR-2011-08-22-894. Norwegian Government, (2011).

Publication 5

Østby, Grethe; Kowalski, Stewart James. (2022) Introducing Serious Games as a Master Course in Information Security Management Programs: Moving Towards Socio-Technical Incident Response Learning. *Handbook of Research on Cross-Disciplinary Uses of Gamification in Organizations.* IGI publishing.


DOI: 10.4018/978-1-7998-9223-6

Publication 6

Østby, Grethe; Kowalski, Stewart James. (2020) Preparing for cyber crisis management exercises. *Augmented Cognition. Human Cognition and Behavior.* Springer.

# Preparing for cyber crisis management exercises

Grethe Østby[1] [0000-0002-7541-6233], Stewart James Kowalski[1] [0000-0003-3601-8387]

[1]Norwegian University of Science and Technology, Gjøvik, Norway

{grethe.ostby;stewart.kowalski}@ntnu.no

**Abstract.** In this paper the authors discuss how to create a preparation schedule for exercises (PSE) to support EXCON-teams and instructors for full-scaled combined crisis management and cyber-exercises. The process to create the preparation schedule starts by performing vulnerability analysis to identify the most relevant and likely threats to the organization, before
processing historical threats and attacks to further focus our simulation scenario development by planning and designing a socio-technical scenario. Moreover, a plan for simulation that are realistic and based on the organization's maturity will be considered, and finally, in terms of a societal crisis impact exercise necessary lectures will be prepared.
After this framework has been reviewed by the HCI International 2020, we plan to test the model when planning for exercises at the Norwegian Cyber Range (NCR) environment. NCR will be an arena where testing, training, and exercise will be used to expose individuals, public and private organizations, government agencies to simulate socio-technical cyber security events and situations in a realistic but safe environment.

**Keywords.** Exercices, cyber exercices, cyber management exercices, cyber crises, cyber crises management exercices

## 1 Introduction

The Norwegian Directorate for Civil Protection (DSB) recommends that full scale crisis management exercises consist of two major components: an exercise directive, and a scenario (DSB, 2016). An exercise directive sets the framework for the exercise, whilst the scenario sets the content and timeline for the exercise.

The *ENISA Good Practice Guide on National Exercises* outlines in the initiation and planning phases of exercises that an organization should prepare an exercise directed to the needs of the organization but does not give guidelines how these needs should be identified (ENISA, 2009).

The authors have from years of experience of planning for crisis management exercises, done vulnerability analysis on the organizations, and prepared and executed lectures beforehand the exercises based on such analyses. Recent research has also

suggested the need to use maturity modelling to prepare for exercises, to plan the exercise for an appropriate level for the participating organizations (Østby & Katt, 2019). Additionally, other recent research suggests preparing scenarios in a socio-technical root cause analytical context to prepare for different types of exercises (Østby, Berg, Kianpour, Katt, & Kowalski, 2019).

By providing a clear step-by-step guide to follow, the authors suggest that such planning framework can provide a more effective and efficient learning environment for exercises.

After the introduction we present background and relevant literature in section 2, before presenting the research approach in section 3. In section 4 we present the suggested preparation schedule for exercises, and in section 5 we conclude and present our future plans on the topic.

## 2 Background and relevant literature

The scope of the authors' research is to investigate information security awareness and cyber security preparedness in society and public organizations like municipalities and counties and to investigate cyber-management in the public emergency organizations in both the organizations themselves and cyber-operations centers. To meet the scope, we will arrange cyber-incidents exercises at the Norwegian Cyber Range (NCR) (NTNU, 2019).

At the NCR, we want to develop and offer near to real life exercises, i.e. full-scaled exercises in a secure environment, to train organizations on strategic, tactical and operational levels together. We plan to copy – paste the organizations socio-technical control structure into a safe environment at the cyber range, and train the teams on system incident handling, incident information escalation and crisis management.

To prepare for such exercises, we plan to test our suggested Preparation Schedule for Exercises (PSE) - framework as presented in this paper. Preparation for cyber exercises often centers around the cyber test bed and a fictive scenario (Micco, Ed, & Rossman, 2002; Vykopal, Vizvary, Oslejsek, Celeda, & Tovarnak, 2017), and the cyber exercises are often executed as competitions (Bei, Kesterson, Gwinnup, & Taylor, 2011; Patriciu & Furtuna, 2009). The author's approach is however, to focus on status in the organization that will be trained, to make the exercise as realistic as possible, but also aligned with the organization's level of awareness and knowledge.

In Jason Kick's Cyber Exercise Playbook (2014), the training audience is divided into 5 different challenge levels, and suggest impact and resolution on how to address the audience based on these challenges. In this paper the author suggests using vulnerability analysis and maturity modelling to find the training audiences/organizations level of expertise or lack of expertise.

System vulnerability analysis involves discovering a subset of the input space with which a malicious user can exploit logic errors in an application to drive it into an insecure state (Sparks, Embleton, Cunningham, & Zou, 2007). Vulnerability analysis in this paper also includes physical/material, social/organization and motivational/attitudinal analysis similar to those presented by Twigg (2001), and will be compa-

rable with Norwegian guidelines for risk – and vulnerability analysis made by The Norwegian Directorate for Civil Protection (DSB) (DSB, 2014). The author also consider Shah and Mehtre's Vulnerability Assessment and Penetration Testing (VAPT) relevant for some organizations of which is competent to consider and relate to such approach (Shah & Mehtre, 2013).

In preparation for full-scale exercises it is also relevant to investigate the organization's experience with crisis in general and cyber-crisis in particular. Additionally, societal trends of which may impact the organization should be considered. To run such investigations, the use of threats - and opportunities analysis can be justified. In a study by Jackson & Dutton (1988) designed to investigate the use of threats and opportunities analysis among decision makers, the authors suggests that managers are being more sensitive to issue characteristics associated with threats than to those associated with opportunities. We suggest however, that by combining threat and opportunity analysis with vulnerability analysis like those previously presented, or together with a vulnerability functional assessment analysis as presented by Depoy et al. (2005), opportunities and vulnerabilities can be presented together.

According to Liao et al., Gartner define Cyber Threat Intelligence (CTI) as "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard" (Liao et al., 2016). Research on managing CTI by CTI-sharing (Brown, Gommers, & Serrano, 2015; Burger, Goodman, Kampanakis, & Zhu, 2014), and use of SIEM's systems to present and evaluate threats (Al Sabbagh & Kowalski, 2015), are relevant practice to consider when preparing for cyber exercises. The authors consider in this paper how to bring this information from ICT-management to the organizations top management to prepare for cyber incidents and exercises which affects the organizations ability to still run their daily business or activity and thereby require top management involvement.

Since the beginning of 2011 DSB has published annual description of possible crisis scenario that could have major impact on Norway (DSB, 2019). There are three major developments in the society, which are presented in the 2019 analysis, and one of these is the security consequences from rapidly increasing digitalization. Such development has led to a number of security analysis and techniques (Mahmood & Afzal, 2013), and it is difficult for organizations which do not have ICT-security as their main tasks, to keep track with these trends. As a preparation for cyber incidents and exercises, the author suggests conducting trend analysis targeting the organizations to be trained as a part of the overall CTI-analysis.

In previous research Østby et al. suggests that socio-technical scenario building can be useful in understanding and defining training scenarios as it gives a good indication on both social and technical challenges from real life cases (Østby, Berg, et al., 2019). A socio-technical system considers both social and technical aspects of change as presented in figure 1.

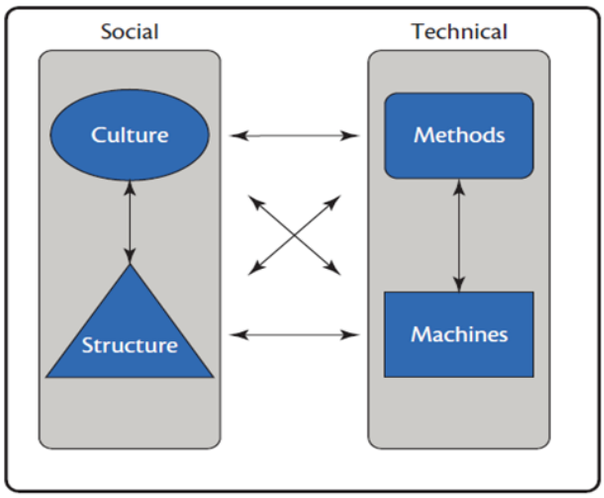



**Fig. 1.** Socio-technical approach (Kowalski, 1994)

In preparation for exercises the socio-technical approach is useful for making scenarios to highlight possible imbalance between the component and may give the organizations directions of how to bring their system back into balance. On the social side of the approach ISO standards like ISO 27005 (ISO 27005, 2018) and ISO 27035 (ISO, 2016) can be used to investigate culture and structure, and on the technical side standards like presented by the Telecommunication Standardization sector of ITU (ITU-T) (ITU-T, 2019) about protection assurance (chapter 5) can be used to investigate the methods and machines in the organization.

Recent research by Walhgren and Kowalski in Sweden indicates that there is a lack of cyber security incident readiness and that most organizations are at such a low level of maturity to deal with information security incidents that it may not even be beneficial for the organization to start off by running full scale exercise (Wahlgren & Kowalski, 2016). Østby & Katt (2019) recently tested Wahlgren & Kowalski's model (Wahlgren & Kowalski, 2016) in the Norwegian Inland Hospital trust, and the results indicated a diversity in needs and knowledge on strategic, tactical and operational layers in the organization.

Van Laere and Lindblom (2018) suggest theoretical education sessions via table-top discussions to role-playing, to give the trainees a fair chance of building skills and confidence before the exercise starts. This is also supported by the authors experience of running crisis management exercises both with and without theoretical lectures beforehand the exercises, and we suggest better learning from the exercise when preparing with lectures.

The Poorvu Center for Teaching and Learning at Yale (Yale, 2019) presents how to write intended learning outcomes from lectures, and suggests that by writing specific, measurable takeaways, learning outcomes improves (Richmond, Boysen, & Gurung, 2016). This is from a cyber security perspective also supported by ENISA's guidelines on assessing key objectives for operators of essential services (OES) and

for the digital service providers (DSP) (ENISA, 2018). The assessment is presented in the order of 1) security measures, 2) questions and 3) evidence.

In this paper we present an adaption of the Backward Design framework, presented by The Porvu Center for Teaching and Learning at Yale (Yale, 2019).

## 3 Research approach

In this paper, we approach the cyber security exercise design and execution challenge by using the design science research in information systems (DSRIS) (Kuechler & Vaishnavi, 2012). Design science research (DSR) is a methodology which can be conducted when creating innovations and ideas that define technical capabilities and product through which the development process of artifacts can be effectively and efficiently accomplished (Kuechler & Vaishnavi, 2012).

How to work on DSR was presented in a thesis written by G. R. Karokola (Karokola, Kowalski, & Yngström, 2011). He visualized this approach as outlined in figure 2.

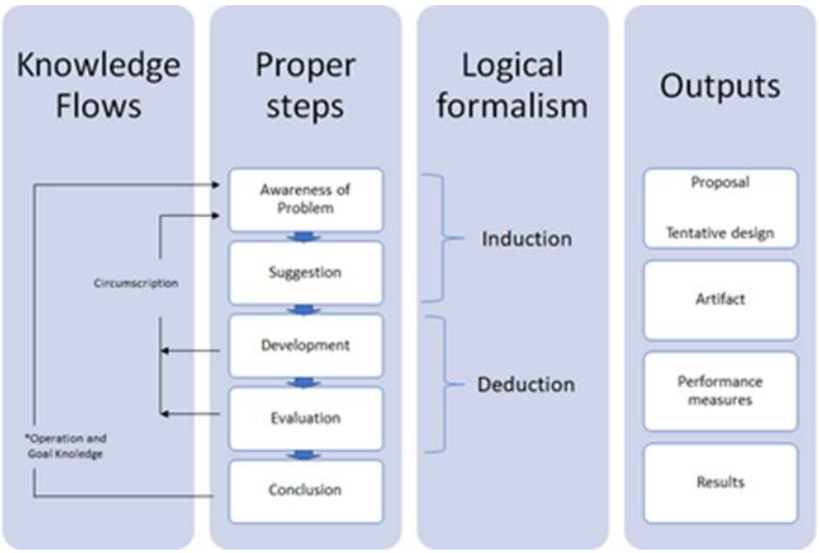



**Fig. 2.** Design research methodology - modified

The main goal of the research is to develop a step by step preparation framework for planning for cyber full-scale exercises.

The authors approach the goal by what can be referred to as a naive inductivist approach. The naive inductivist approach starts by first observing a phenomenon and then generalizing about the phenomenon which leads to theories that can be falsified or validated (Kowalski, 1994).

Our proposed artifact in this paper is a framework to prepare for exercises which involves

1) vulnerability analysis to identify the most relevant and likely threats to the organization, both from an overall perspective and those specific to the organization,

2) work with the cybersecurity teams to understand historical threats and attacks to further focus our relevant simulation scenario development,

3) plan and design a socio-technical scenario for the exercise,

4) plan for simulation that are realistic and based on the organization's maturity,

5) and finally, in terms of a societal crisis impact exercise; look into the organization's responsibility (laws and regulations), crisis management roles and responsibilities, and suggested escalation continuity plans (involving information continuity plans), to prepare for exercise lectures.

## 4 Preparation schedule for exercises (PSE)

The proposed artifact is based on relevant literature presented and practical experience in planning for exercises. In this section we present the five-step preparation schedule for exercises (PSE) for full-scale cyber-incident exercises that will be executed for both strategic, tactical and operational participants from the organizations that are being trained.

### 4.1 Vulnerability analysis

To identify the most relevant and likely threats to the organization, both from an overall perspective and those specific to the organization, the authors suggest using an overall SWOT-analysis (strengths and weaknesses, opportunities and threats) together with information from SIEMS systems and systems architecture overviews. Additionally, we want to investigate existing risk- and vulnerability analysis or prepare such if none exist. The suggested vulnerability analysis is presented in figure 3.

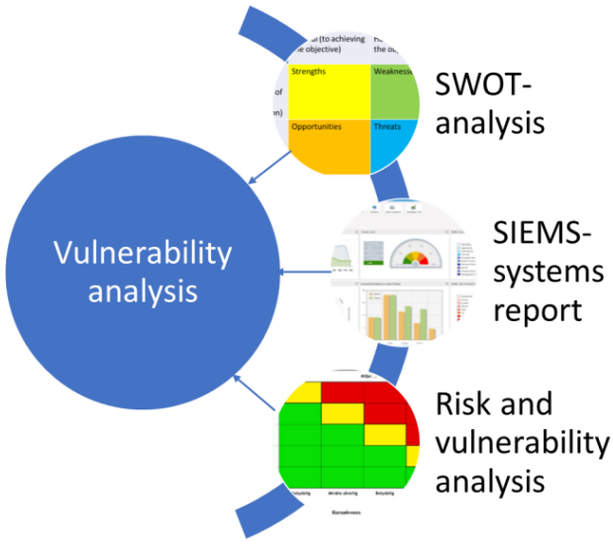



**Fig. 3**. Vulnerability analysis before exercises

We also suggest executing penetration testing as a part of the vulnerability analysis before exercises. Such reports will outline all the system and cyber vulnerabilities in a more detailed context and will give the organization more detailed results to work with after the exercise.

### 4.2 Historical threats and attacks

To approach analysis of historical threats and attacks both from within and from the outside of the organization, the authors suggests implementing reporting escalation processes from Security Incident and Event Management Systems (SIEMS) - to improve information flow and indicate what relevant information should be provided from a cyber incident to the crisis information management systems used.

In future research, a socio-technical escalation framework (STEF) to support synchronizing Security Incident and Event Management Systems (SIEMS) and Crisis Information Management Systems (CIMS) as suggested in Østby, Yamin and AlSabbagh (2019) could be implemented.

It is also important to evaluate trends in threats both within the organization and in the society in a national and international context similar to the DSB's incidents analysis (DSB, 2019).

### 4.3 Socio-technical scenario building

In Østby, Berg, et al. (2019), different socio-technical models are suggested for different types of exercises. In our planning for exercises at the NCR, we will test how

this approach works compare them to other scenario-building models. The socio-technical models, however, needs measurement standards when setting up the scenarios. We intend to use learning outcomes as described in section 4.5 as measurement. We want to use ISO-standards to measure the status of the social part of the organization, and the ITU-T-standards to measure the technical part of the organization. Our approach can be visualized like presented in figure 4.

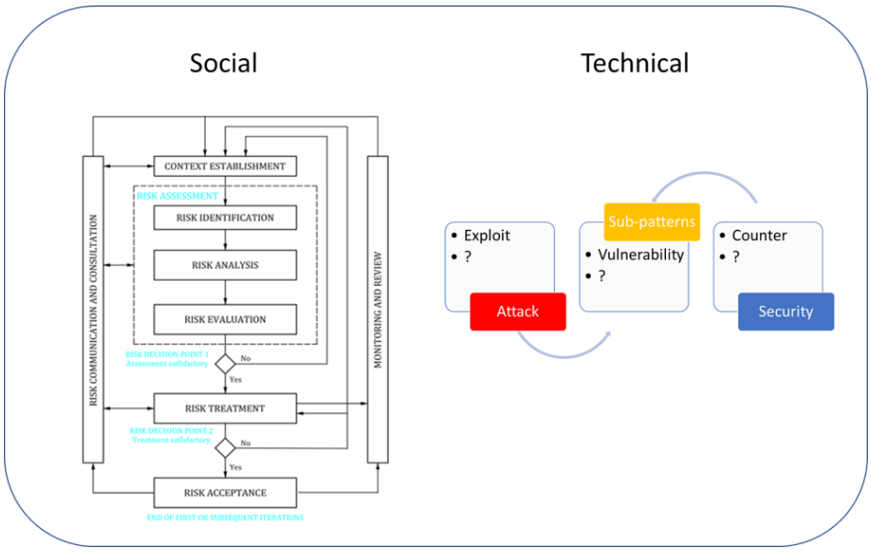



**Fig. 4**: Socio-technical standardization scenario measurement

The scenario will combine the results from the social and technical measurements to provide a total-concept scenario for the full-scale exercises. By this approach it will be possible to also measure the scenario incident handling process during the exercise.

### 4.4 Escalation maturity analysis

When analyzing the mentioned maturity escalation study executed at the Inland Hospital trust in Norway (Østby & Katt, 2019), the authors focused on the weakest scores. However, the authors suggest that it is also important to focus on the high scores, to find the organization's strengths, and find the prioritization to the management to find an action strategy within the regulations of crisis management in the organization.

This is especially important when preparing for the exercise, to give the participants the possibility to perform successfully on their strengths. In planned research we want to suggest improvement-work during and after the exercise (Østby & Katt, 2019).

It is however important to give the participants the possibility to train on their maturity weaknesses, and when preparing for the exercises, there will be a need to pro-

vide suggestions on how to handle the organizations biggest challenges on both strategic, tactical and operational layers. This process can be presented as in figure 5.

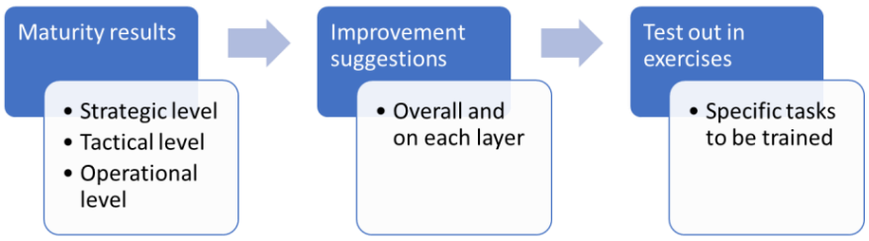



**Fig. 5.** Maturity results to be trained

For the exercise itself it can be organized with time-outs when these specific tasks are put in focus. That is, time to reflect on specific tasks and to document lessons learned experiences.

### 4.5 Lectures

In an evaluation after a recent table-top exercise for the tactical/emergency ICT-management team at our university, most of the participants answered relevant, very relevant and huge relevance when asked about relevance in lectures beforehand the exercise. The results are presented in table 1.

**Table 1.** Relevance in lectures beforehand exercises[1]

| | No relevance | Some relevance | Relevant | Very relevant | Huge relevance |
|---|---|---|---|---|---|
| Regulations in security and emergency at Universities and Colleges (laws, regulations and guidance's), and other tasks crises management should be prepared for. | 0% | 16,7% | 50% | 16,7% | 16,7% |
| Crisis management and work in crisis staff: Situational analysis, need of recourses (personnel and material), roles in crises and operative management. | 0% | 0% | 33,3% | 50% | 16,7% |

[1] 6 out of 10 participants answered the evaluation form

| | | | | | |
|---|---|---|---|---|---|
| Information in emergencies, crisis management brief, crises communication and CIM. | 0% | 0% | 16,7% | 66,7% | 16,7% |
| Emergency plans, task lists for roles in crisis (critical analysis of the team's emergency plan). | 0% | 0% | 33,3% | 50% | 16,7% |

When planning the lectures for the organization participating in exercises at the Norwegian Cyber Range, it will be necessary to plan the lectures to support both the strategic, tactical and operational teams. However, the focus in the lectures will still be responsibilities, roles and escalation procedures. In this research we suggest preparing lectures as executed in this mentioned exercise, of which is a modified version of Backward Design, in a socio-technical context, as presented in figure 6.

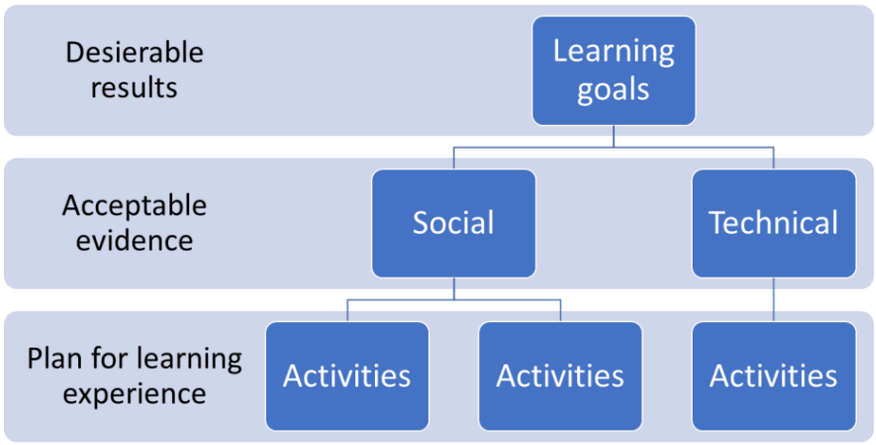



**Fig. 6:** Backward Design, modified in a socio-technical context (Wiggins, Wiggins, & McTighe, 2005)

By using this approach, the learning experience may flow into the exercise. That is that we don't need to "stop" the lectures when starting the exercise, as much of the learning experience will take place in the actual exercise in so called teachable moments.

## 5 Conclusion and future research

In this paper the author discusses a work in progress, to create a preparation schedule for exercises (PSE) to support exercise control (EXCON) teams and instructors for full-scaled combined crisis management and cyber-exercises.

After this framework has been reviewed and presented at the HCI International 2020 we plan to implement, test and evaluate the framework when setting up cyber crises exercises in the Norwegian Cyber Range (NCR) environment. We shall test the relevance of the framework for different types of organizations in Norwegian public sector and help develop interoperability standards so that scenario and exercises can be exchange both with in Norway and around the world.

## 6 References


Al Sabbagh, B., & Kowalski, S. (2015). *MULTIDISCIPLINARY SECURITY*. Retrieved from www.computer.org/security

Bei, Y., Kesterson, R., Gwinnup, K., & Taylor, C. (2011). *CYBER DEFENSE COMPETITION: A TALE OF TWO TEAMS* *.

Brown, S., Gommers, J., & Serrano, O. (2015). From cyber security information sharing to threat management. In *WISCS 2015 - Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, co-located with: CCS 2015* (pp. 43–49). Association for Computing Machinery, Inc. https://doi.org/10.1145/2808128.2808133

Burger, E. W., Goodman, M. D., Kampanakis, P., & Zhu, K. A. (2014). Taxonomy model for cyber threat intelligence information exchange technologies. In *Proceedings of the ACM Conference on Computer and Communications Security* (Vol. 2014-November, pp. 51–60). Association for Computing Machinery. https://doi.org/10.1145/2663876.2663883

Depoy, J., Phelan, J., Sholander, P., Smith, B., Varnado, G. B., & Wyss, G. (2005). *RISK ASSESSMENT for PHYSICAL AND CYBER ATTACKS on CRITICAL INFRASTRUCTURES*.

DSB. (2014). *Veileder til helhetlig risiko og sårbarhetsanalyse i kommunen*. Retrieved from https://www.dsb.no/globalassets/dokumenter/veiledere-handboker-og-informasjonsmateriell/veiledere/veileder-til-helhetlig-risiko-og-sarbarhetsanalyse-i-kommunen.pdf

DSB. (2016). *VEILEDER I PLANLEGGING, GJENNOMFØRING OG EVALUERING AV ØVELSER Metodehefte: Fullskalaøvelse*.

DSB. (2019). *Analyser av krisescenarioer*. Retrieved from https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf

ENISA. (2009). *Good Practice Guide on National Exercises Enhancing the Resilience of Public Communications Networks Good Practice Guide on Exercises 2 Good Practice Guide on National Exercises*. Retrieved from http://www.enisa.europa.eu/act/res

ENISA. (2018). Guidelines on assessing DSP and OES compliance to the NISD security requirements. https://doi.org/10.2824/265743

ISO. (2016). *ISO 27035 - 1*. Retrieved from https://www.standard.no/nettbutikk/sokeresultater/?search=ISO+27035&subscr=1

ISO 27005. (2018). *ISO 27005*. Retrieved from www.iso.org

ITU-T. (2019). *ITU-T FG-DFC TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU Protection assurance use case for a payment transaction Security Working Group Deliverable Focus Group Technical Report*. Retrieved from https://www.itu.int/en/ITU-T/focusgroups/dfc/Documents/DFC-O-009_Security deliverable_Report_Protection Assurance Use Case for a Payment transaction.pdf

Jackson, S. E., & Dutton, J. E. (1988). *Discerning Threats and Opportunities*. *Source: Administrative Science Quarterly* (Vol. 33).

Karokola, G., Kowalski, S., & Yngström, L. (2011). Secure e-government services: Towards a framework for integrating IT security services into e-government maturity models. In *2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference*. https://doi.org/10.1109/ISSA.2011.6027525

Kick, J. (2014). *Cyber Exercise Playbook*.

Kowalski, S. (1994). *IT Insecurity: A Multi-disiplinary Inquiry*. Stockholm University.

Kuechler, W., & Vaishnavi, V. (2012). *A Framework for Theory Development in Design Science Research: Multiple Perspectives*. *Journal of the Association for Information Systems* (Vol. 13).

Liao, X., Yuan, K., Wang, X., Li, Z., Xing, L., & Beyah, R. (2016). Acing the IOC game: Toward automatic discovery and analysis of open-source cyber threat intelligence. In *Proceedings of the ACM Conference on Computer and Communications Security* (Vol. 24-28-October-2016, pp. 755–766). Association for Computing Machinery. https://doi.org/10.1145/2976749.2978315

Mahmood, T., & Afzal, U. (2013). *Security Analytics: Big Data Analytics for Cybersecurity A Review of Trends, Techniques and Tools*. 2nd National Conference on Information Assurance (NCIA). Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6725337

Micco, M., Ed, D., & Rossman, H. (2002). *Building a Cyberwar Lab: Lessons Learned. Teaching cybersecurity principles to undergraduates*. Retrieved from http://penguin.nsm.iup.edu/security.

NTNU. (2019). The Norwegian Cyber Range. Retrieved from https://www.ntnu.no/ncr

Østby, G. ;, Berg, L. ;, Kianpour, M. ;, Katt, B. ;, & Kowalski, S. (2019). A Socio-Technical Framework to Improve cyber security training: A Work in Progress. Retrieved from https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2624957

Østby, G., & Katt, B. (2019). Maturity modelling to prepare for cyber crisis escalation and management. Retrieved from https://orcid.org/0000-0002-7541-6233

Østby, G., Yamin, M. M., & Asabbagh, B. (2019). SIEMS in Crisis Management: Detection, Escalation and Presentation – A Work in Progress. Retrieved from

https://www.researchgate.net/profile/Stefan_Suetterlin/publication/334139727_Team_learning_in_cybersecurity_exercises/links/5d1a241e299bf1547c8eec06/Team-learning-in-cybersecurity-exercises.pdf#page=40

Patriciu, V.-V., & Furtuna, A. C. (2009). Guide for Designing Cyber Security Exercises. In *WSEAS International Conference on Information Security and Privacy*. WSEAS Press. Retrieved from http://www.wseas.us/e-library/conferences/2009/tenerife/EACT-ISP/EACT-ISP-28.pdf

Richmond, A. S., Boysen, G. A., & Gurung, R. A. R. (2016). *AN EVIDENCE-BASED GUIDE TO COLLEGE AND UNIVERSITY TEACHING*.

Shah, S., & Mehtre, B. M. (2013). *A Modern Approach to Cyber Security Analysis Using Vulnerability Assessment and Penetration Testing*. *International Journal of Electronics Communication and Computer Engineering* (Vol. 4). Retrieved from www.ijecce.org

Sparks, S., Embleton, S., Cunningham, R., & Zou, C. (2007). Automated vulnerability analysis: Leveraging control flow for evolutionary input crafting. In *Proceedings - Annual Computer Security Applications Conference, ACSAC* (pp. 477–486). https://doi.org/10.1109/ACSAC.2007.27

Twigg, J. (2001). *SUSTAINABLE LIVELIHOODS AND VULNERABILITY TO DISASTERS*. *Disaster Management Working Paper* (Vol. 2).

van Laere, J., & Lindblom, J. (2018). Cultivating a longitudinal learning process through recurring crisis management training exercises in twelve Swedish municipalities. *Journal of Contingencies and Crisis Management*. https://doi.org/10.1111/1468-5973.12230

Vykopal, J., Vizvary, M., Oslejsek, R., Celeda, P., & Tovarnak, D. (2017). Lessons Learned From Complex Hands-on Defence Exercises in a Cyber Range. In *FIE Frontiers in Education*.

Wahlgren, G., & Kowalski, S. (2016). A Maturity Model for Measuring Organizations Escalation Capability of IT-related Security Incidents in Sweden. *Assosiation for Information Systems*.

Wiggins, G., Wiggins, G. P., & McTighe, J. (2005). *Understanding by Design*. ASCD. Retrieved from https://books.google.no/books?hl=no&lr=&id=N2EfKlyUN4QC&oi=fnd&pg=PR6&dq=Wiggins+GP,+McTighe+J.+(2005).++Understanding+by+Design.&ots=gpcyn4UH5x&sig=HmWITitQ3nVTu1XKcvtKGTibJfA&redir_esc=y#v=onepage&q&f=false

Yale. (2019). Intendent learning outcomes. Retrieved from https://poorvucenter.yale.edu/IntendedLearningOutcomes

Publication 7

Østby, Grethe; Lovell, Kieren N.; Katt, Basel. (2020) EXCON Teams in Cyber Security Training. 2019 *International Conference on Computational Science and Computational Intelligence (CSCI).* IEEE.

Publication 8

Østby, Grethe; Berg, Lars; Kianpour, Mazaher; Katt, Basel; Kowalski, Stewart James. (2019) A Socio-Technical Framework to Improve cyber security training: A Work in Progress. *CEUR Workshop Proceedings. vol. 2398.*

# A Socio-Technical Framework to Improve cyber security training: A Work in Progress

Grethe Østby[1[0000-0002-7541-6233]], Lars Berg[2[0000-0001-8688-5759]], Mazaher Kianpour[1[0000-0003-2804-4630]], Basel Katt [1[0000-0002-0177-9496]], Stewart Kowalski[1 [0000-0003-3601-8387]],

[1] Norwegian University of Science and Technology, Postboks 191, 2802 Gjøvik
[2] Telenor Norge AS, Snarøyveien 30, 1331 Fornebu

lncs@springer.com

**Abstract.** In this paper we discuss a work in progress to create a socio-technical system design framework for cyber security training exercises (STSD-CSTE) to support the development of cyber security training in the Norwegian Cyber Range (NCR). The process to create the framework started by first performing a socio-technical systems root cause analysis of an Advanced Persistent Threat (APT) incident called "Operation Socialist". Operation Socialist was the code name given by the British signals and communications agency Government Communications Headquarters (GCHQ) to an operation in which they successfully breached the infrastructure of the Belgian telecommunications company Belgacom (now Proximus Group) between 2010 and 2013. To extract relevant information from the case four socio-technical systems models were tested. The four models integrated into one framework were the Cassano-Piche Structural Hierarchy model, the "Security by Consensus" model, the Kowalski's Socio-Technical systems dynamic model and the Withword's 8 criterial model. After this framework has been reviewed by the socio-technical research community we plan to test the framework with exercises in the Norwegian Cyber Range environment. NCR will be an arena where testing, training, and exercise will be used to expose individuals, public and private organizations and government agencies to simulate socio-technical cyber security events and situations in a realistic but safe environment.

**Keywords:** Socio-technical models; Root cause analysis, Crisis-management, Cyber Security simulations, scenario exercises

## 1 Introduction

According to the Cisco 2018 annual Cyber Security report, the lack of trained cyber security personnel is one of the key issue challenging security management (Cisco, 2018). This lack of trained personnel is not a new problem. In 2017, 27 percent cited the lack of talent as a major obstacle, compared with 25 percent in 2016 and 22 percent in 2015. The gap between supply and demand for trained security personnel is growing.

In this paper, we outline our work in progress at the Norwegian Cyber Range to help fill this competence gap by using socio-technical models to construct training exercises

and scenarios based on actual cyber incidents. In our work, we are attempting to combining socio-technical theory with didactic theory and crisis management training practices to cyber education and training.

The paper is structured as follows: After the introduction and background in section 1 and 2, in section 3 our research approach is discussed, together with our framework for building scenarios and exercises in cyber readiness based on real life incidents. In section 4, we review relevant literature. Then, in section 5 we present the case and one example of how we used socio-technical models to analyze the case, and in section 6 we exemplify the outcome of this application. In section 7 we end this paper by outline our prospects for further research.

## 2 Background

Several threat-actors are focusing on telecom services and infrastructure. According to Norwegian National Security Authority (NSM) in 2017 the NorCERT alarm on critical national infrastructure were triggered more than 22.000 times and more than 5.200 Norwegian entities were subject to advanced cyber-attacks (NSM, 2018). In the period May 2016 to May 2017 Telenor Norway managed 1800 cyber intrusion attempts in own and customers networks (Telenor, 2018). Private and public entities are facing new cyber threats day by day, and threat actors have different motivations. The most advanced cyber-attacks are often referred to as Advanced Persistent Threat (APT). Li defined APT as a cyber-attack launched by a group of sophisticated, determined, and coordinated attackers who systematically compromise the network of a specific target or entity for a prolonged period (Li, Lai, & Ddl, 2011). APTs have capacity, capability and motivation to run clandestine operations for months and years to achieve their objectives. Most organizations are not prepared to handle those kinds of advanced malicious cyber-attacks, and when it happens the repercussions are vast.

Detecting anomalies that occur only within individual variables is often trivial, while detecting correlation anomalies is much harder and is practically important in fault analysis of complicated dynamic systems (Idé, Lozano, Abe, & Liu, 2013). In a complex cyber-physical system, such as a smart grid, while some of the relationships between time series can be directly observed, other mutual dependencies are significantly complex to extract computationally. A typical cyber-physical system may include multiple process series with hundreds of mutual dependencies, where many of them are not directly observable (Rahman, Momtazpour, Zhang, Sharma, & Ramakrishnan, 2015).

To understand and manage cyber security situations, we suggest using socio-technical models to prepare for training and education based on real-life incidents. A sociotechnical system (STS) is the synergistic combination of humans, machines, environments, work activities and organizational structures and processes that comprise a given enterprise (Carayon et al., 2015). The goal of STS is a comprehension and accounting for the 'joint optimization of the social and technical systems', i.e. the different subsystems or different system components. Workers adapt to the sociotechnical system, but, in their turn, also serve to adapt the sociotechnical system itself.

## 3 Research Approach

In this paper, we approach the cyber security challenges using what can be referred to as a naive inductivist approach. The naïve inductivist approach starts by first observing a phenomenon and then generalizing the phenomenon which leads to theories that can be falsified or validated (Kowalski, 1994). This approach will use the methodology outline by design science research in information systems (DSRIS) (Kuechler & Vaishnavi, 2012). This methodology uses artifact design and construction (learning through building) to generate new knowledge and insights into a class of problems.

DSRIS requires three general activities: (1) construction of an artifact where construction is informed either by practice-based insight or theory, (2) the gathering of data on the functional performance of the artifact (i.e., evaluation), and (3) reflection on the construction process and on the implications the gathered data (from activity (2)) have for the artifact informing insight(s) or theory(s) (Kuechler & Vaishnavi, 2012).

How to work on these steps was presented in a thesis written by Karokola (Karokola, 2012). He visualized this approach as outlined in figure 1. As we are approaching our work in a naive inductivist approach, we modified the logical formalism in the model from abduction to induction.

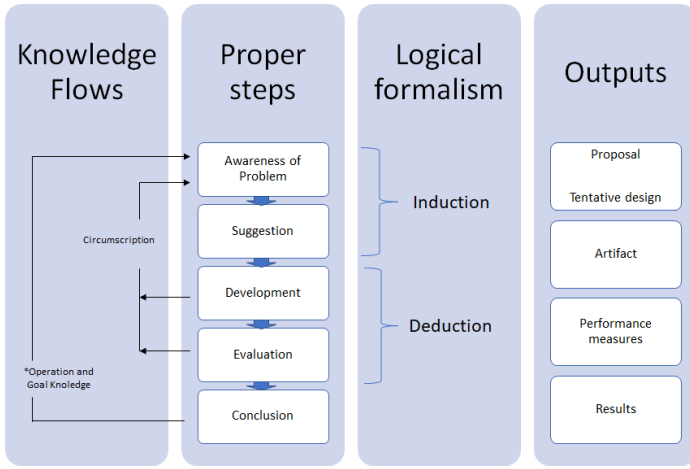



Figure 1, Design research methodology - modified

To propose an artifact in an inductive approach we started up by analyzing an actual cyber-incident to present the problem (first step in the 2nd column). For the next step in this work in progress paper we suggest a model based to deal with the problem in crisis management education in which different kind of exercises are needed to target different aspect in a socio-technical security system (second step in the 2nd column). The goal of the paper is to propose a tentative design (first step in the 4th column), in which we want to test when preparing for cyber exercises at the Norwegian Cyber Range.

### 3.1 Apply an Actual Incident Case study

The actual incident we chose for our first attempt to design a framework was the APT-attack "Operation Socialist" making international headlines in September 2013. Operation Socialist was the code name given by the British signals and communications agency Government Communications Headquarters (GCHQ) to an operation in which they successfully breached the infrastructure of the Belgian telecommunications company Belgacom (now Proximus Group) between 2010 and 2013.

We did a root cause analysis on this incident using four different socio-technical models. Those models were chosen based on the different approaches they have, to see if any or all of them could be relevant for making scenarios for exercises.

The responsible of the technical operations are often considered to be within the organization. However, most organizations today are complex and cannot perform all technical tasks by themselves. By entering into contracts and service level agreement of various sort, the companies have other people and organizations to run their technical operations and are therefore bounded by agreements and thereby regulations. Withford & Zaic describe four different system levels to analyze requirements for technical operation with WOSP (Web of System Performance) (Whitworth & Zaic, 2018): Hardware requirements, software requirements, human requirements and communal requirements. They define WOSP as a theoretical framework for the balanced design and evaluation of advanced information systems. The framework analyses performance via four fundamental system elements: Boundary, internal structure, effectors and receptors. As this is organizational issue, we considered this model relevant when designing scenarios for discussion exercises.

The four quadrants used in the proposed framework are modeled after the naive socio-technical system dynamic mental model proposed by Kowalski (Kowalski, 1994). Kowalski's mental model attempts to describe how systemic security weaknesses in socio-technical systems can be analogized as homeostatic imbalance. Homeostatic imbalance is the disability of the internal environment to remain in equilibrium in the face of internal, external and environmental changes (Pelletier, Guertin, Paige Pope, & Rocchi, 2016). Homeostatic imbalance is a concept that we suggest can also be used with scenario building to model the inability of an organization to face internal and external cyber threats.

The Security by Consensus model (SBC), is a model that attempt to capture the static and dynamic characteristics of ICT systems security (Kowalski, 1994). Moreover, the model sub-divides security measures into subclasses. The holistic approach required the issue of IT crime be examined, and the model was used to make computer abuse reports. Such reports are relevant on the strategic level and as a method to define action points in the organizations, and thereby likely to be relevant for table-top scenarios.

In the Norwegian Cyber Range project, we also plan to run full-scale exercises in Norway. Cassano-Piche et. al. Socio-technical systems analysis of the BSE Epidemic in the UK using the Rasmussen framework helped vertically integrate a socio-technical root cause analysis of Mad Cow Diseases across multiple levels and hierarchies of socio-technical system in the United Kingdom as a whole (Cassano-Piché, Vicente, & Jamieson, 2006). Consequently, we believe it can be used to design scenarios for large scale cyber security incidents and events in Norway.

Suggested modelling four quadrants used in the proposed framework are modeled after the naive socio-technical system dynamic mental model proposed d by Kowalski (Kowalski, 1994). As mentioned before, homeostatic imbalance concept can be used with scenario building. Therefore, the model suggested consists of the four socio-technical aspects suggested by Kowalski (Kowalski, 1994):

Table 1: Socio-technical aspects

| | |
|---|---|
| Social | Structure |
| | Culture |
| Technical | Machine |
| | Methods |

First, we tried to see where scenarios for **exercises** could fit our socio-technical model. There are several types of exercises, and in this paper, we have used the exercise-definitions outlined by the Norwegian Directorate for Civil Protection (DSB): discussion exercises, functional exercises, simulation exercises and full-scaled exercises. A *discussion exercise* is executed under different kind of names, for example, table-top, dilemma-exercises or seminar-exercises (DSB, 2016b, 2016c, 2016d, 2016a). In a discussion exercise, all participants gather in one room and all communication happens within this room. Inputs are given oral or on paper/screen/canvas sheets. All activity is to focus around discussion on concept and ideas and no concrete action or communication outside the exercise is needed. The participants are not to play or simulate, but to discuss specific and generic problems related to the scenario presented by the instructor. *Function exercises* is a collective name for exercises that test one or more functions within the organization (DSB, 2016b). It might be technique, organization or capabilities. Attending a function exercise, it is more about what to exercise than how the exercise is done. Function exercises are also referred to as procedure exercises. *A simulation exercise* consists of two elements: The attenders and the simulation counterparts (DSB, 2016d). A simulation exercise can be illustrated as if the game is running within a "closed bubble", where the participants are staying in the inner bubble and the counterparts surrounding them. The participants will normally stay in their accustom premises, with their normally accessible tools and equipment. The simulation counterparts are staying in other premises, and control the game based on a planned scenario. The purpose is to convey a message with a certain effect to the participants. *A full-scale exercise* consists of all the elements in a simulation exercise, and functions, normally on a tactical level doing practical work (DSB, 2016a). A full-scale exercise is always real time. You use the same equipment as you normally have access to, and exercise in the places you normally are working.

For each kind of exercise, we need **relevant scenarios**. A scenario is a summary of the plot of a play, including information about its characters, scenes, or a predicted sequence of events (The free dictionary, by Farlex). The common way of making scenarios is to find out who is participating in the exercise and make the scenario relevant for the participants. For example, in 2017, a group from NTNU, CCIS, The Norwegian Cyber Defence and the Norwegian Civil Defence made a table-top cyber exercise for the Oppland County Office management group and for the county readiness council. We made the scenario based on the participants and their responsibility. The scenario

was based on what can happen in the society more than what has happened, and it was all made up by ideas. As a reflection after the exercise we asked ourselves if there are relevant theories to approach these kinds of scenarios in a better way, and we could not find any relevant theories on this specific matter.

Large companies have a similar approach for creating scenarios to run exercises. Telenor is running annual full-scale cyber exercises including participants and observers from the Norwegian Armed Forces, The Norwegian Police, The Norwegian National Security Authority and other invited participants. The scenarios are meant to reflect true-to-life cyber incidents the organization faces and put the participants to the test. Experiences and lessons learned build operational, tactical and strategic competence and improve the participant's organizations in facing and managing cyber security incidents. Telenor has similar idea-based approach for making scenarios for exercises.

By considering either Structure, Methods, Machines or Ethical/Legal i.e. culture in the scenario for exercise build, we can determine where different exercises would be useful. Moreover, by having performed a root cause analysis and thus determined the underlying "real", that is major and sine qua non - reasons for the cyber-attack, building an appropriate scenario based on this could prove more accurate, give higher learning quality/effect and more cost effective.

To exemplify this approach, we have discussed the NATO exercise Trident juncture executed in and hosted by Norway in 2018. The main scenario was made for the full-scale exercise within a 3-week timeline. The strategic part of the exercise was kept outside the full-scale exercise and started instead at the end of the full-scale exercise timeline. The scenario for the strategic part of the exercise was in this case based only on structure and methods. The scenario for the NATO exercise would in this case be placed both in an overall context in the model, but the strategic part of the exercise would be placed in the upper right part of the model.

When planning for the annual exercise at the Oppland county readiness council in 2017, the exercise's theme was a cyber-attack against municipalities ICT-systems (Oppland Arbeiderblad, 2017). The county readiness council was given step-by-step information about the scenario and had round table discussions based on those inputs. The discussions were based on the structure in the organizations, laws and regulations and ethical issues (amongst others) – a typical discussion exercise that would be placed in the upper left corner in our model.

When testing systems such as fire alarm systems, it requires a certain methodology and actual use of machines. Fire-alarm exercises is typical functional exercises and you will be placed in the lower right corner in our model. Other known exercises that is based on methodology and machines is cyber mega games, better described as simulation games.

When analyzing the outlined DSB's definitions of exercises, we found that there is not any definition on cultural and machine exercises (lower left corner of our model). However, there are examples of real-life incidents which has been used in teaching strategic and ethical exercises, such as the Therax-25 case (Computing Cases, 1983). We consider this as an area of which can be developed better in combining exercise-definitions and scenarios and have presented this in our future research chapter.

Our scenario for exercise perception is shown in figure 2.

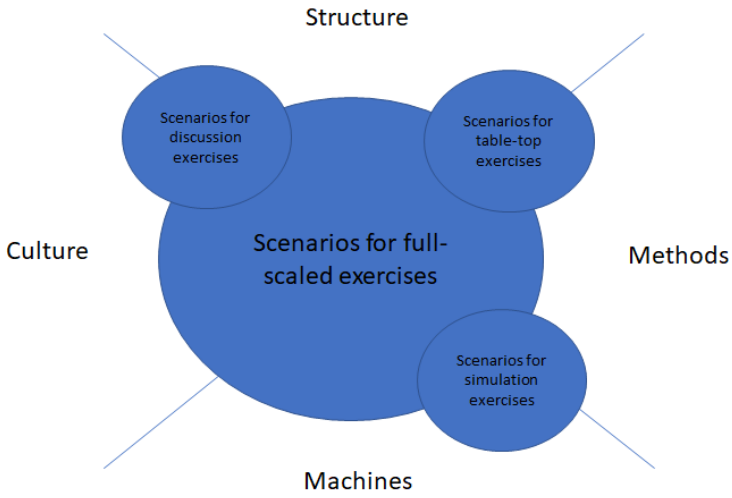



Figure 2: Placing different scenarios for exercises in a social-technical context

## 4 Relevant literature

Today we witness rapid developments of APT tools and systems. Future scenarios include attack vectors orchestrating sets of APT tools in mixed interaction with networks of military units and civilian infrastructures. Carlsson & Gustavsson state that we must prepare ourselves to cope with these threats through awareness and education (Carlsson & Gustavsson, 2018).

Most organizations are not prepared to handle the vast implications of these crises. A challenge in crises is to transfer the accumulated knowledge flowing from concrete experiences, well-documented by crisis management researchers, to learning models in which organizational actors will be **actively engaged**. One of the avenues to better integrate this learning can be found in organizational development approaches (Lalonde, 2007).

Since the start of the 1980s, the field of crisis management has been characterized by two main trends: planning in crisis management and the analysis of organizational contingencies during a crisis (Lalonde, 2007). Based on vast relevant research on crisis management, Lalonde created a synthesis of results from academic research and classified the results with reference to:

- types or contents of lessons, returning to the question *what have we learned?*, whether new information, the consolidation of existing organizational routines stemming either from crisis plans or routines learned within

the organization, or tacit knowledge coming from socialization in a trade or profession or from an organizational cultural environment, etc.;
- learning conditions, returning to the question how or in what conditions *did we learn?*, including experimentation in real time in "real" situations, simulations of the experience, training, confrontation and sharing of experiences, etc.;
- the potential to transfer knowledge within the organization, aiming to respond to the question how can we incorporate this knowledge in an organizational learning model?

In our ongoing research, we use an actual APT-attack to extract the consequences from the attack and figure out what we can learn from such attacks, and how to implement lessons learned in exercises enable also other organizations learn from it.

Scenarios are tools for improving the decision-making process on a background of possible future environments. The scenarios should not be treated as predictions capable of influencing the future nor science fiction stories prepared merely to titillate the imagination (Schoemaker & van der Heijden, 2008). In a study to describe how scenarios used in an environmental science program function in terms of the type of questions they evoked, the results gave that questioning in different ways all bring learning to participants (Dahlgren & Öberg, 2001).

# 5 Case background and example

## 5.1 Operation Socialist

Belgacom operates a substantial number of data links internationally and it serves millions of people across Europe as well as officials from top institutions including the European Commission, the European Parliament, the European Council and the NATO HQ Europe. When Belgacom's internal security team began to suspect that their system was infected with a virus, they hired in outside experts, and after a while the Belgian military intelligence to handle the situation (Marquis-Boire, Guarnieri, & Gallagher, 2014). Some anomalies where detected already in 2012, but Belgacom's security team was unable to identify the cause.

The operation's existence were revealed in documents leaked by the former National Security Agency contractor Edward Snowden in 2013. The malware disguised as legitimate Microsoft software, where identified as the source of the problems. The leakage stated that it was the Government Communications Headquarters (GCHQ) who had infiltrated Belgacom's systems. GCHQ is the British intelligence and security organization responsible for providing signals intelligence (SIGINT) and information assurance to the government and armed forces of the United Kingdom. According to the leaked documents, from Snowden, GCHQ had probed Belgacom's infrastructure for years. Additionally, the documents suggested that Operation Socialist had been recognized by the head of the GCHQ's Network Analysis Centre as a success. Snowden subsequently described Operation Socialist as the "first documented example to show one EU member state executing a cyber-attack on another…" (Marquis-Boire et al., 2014).

According to the leakage, GCHQ had been able to get access to vital data within the mentioned organizations. This led to both political and organizational difficulties for multiple stakeholders.

GCHQ had allegedly used Quantum Inserts technology to target Belgacom and GPRS roaming exchange (GRX) providers like the Comfone, Syniverse, and Starhome. Quantum Insert is the process of injecting TCP sessions into a TPC stream and sending the victim in the wrong direction towards a malicious website that infects their computers with malware at lightning pace (Marquis-Boire et al., 2014). The combination of an IP address and a port is strictly known as an endpoint and is sometimes called a socket. A TCP connection is defined by two endpoints a.k.a. sockets. The Quantum Insert attack started by finding that way into the Belgacom systems by targeting their engineers use of passwords on LinkedIn (Marquis-Boire et al., 2014), the APT kill-chain was as follows:

- Reconnaissance: The APT choose targets of interest and surveil for a period their use of services on the internet, i.e. Belgacom system administrators active on LinkedIn.
- First stage: Drivers which act as loaders for a second stage. When started loading, loads and executes stage 2.
- Second stage: When launched it cleans traces of the initial loader, and then loads the next part and monitors its execution (NB! May disinfect by failure).
- Orchestrator: Service orchestrator working in Windows' kernel. Loads the next part of the malware.
- Information harvesters: Include data collectors, self-defense engine, functionality for encrypted communications, network capture programs, and remote controllers of different kinds.
- Stealth implants: *Pointers* that reference specific locations in memory. Difficult to find, as it is very much alike pool scanning from kernel memory (used by Windows).

Technically Quantum Inserts are categorized as “man-on-the-side attacks” which is a subcategory to “waterhole attacks”. As such APT-attacks are very difficult to discover, the exact time of when the stealth implants were in place is uncertain, but the investigators suggested an approximately startup in 2010. The Intercept summered up the story timewise in 2018 (Gallagher, 2018). The timeline of the incident is shown in figure 3.

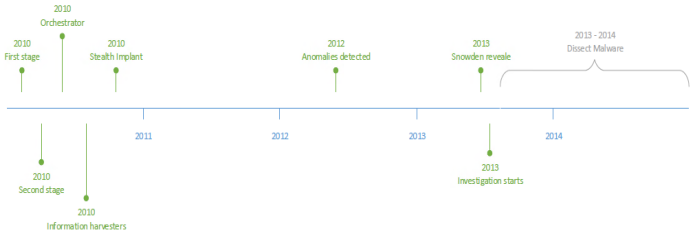



Figure 3: Quantum Insert escalation and period of detection, investigation and dissection

### 5.2 Example

One of the models we used for analyzing the case was the BSE Structural Hierarchy model based on Rasmussen structural hierarchy model (Cassano-Piché et al., 2006). In this paper it is presented as an acci-map. An acci-map is a systems-based technique for accident analysis, specifically for analyzing the causes of accidents and incidents that occur in complex Socio-technical systems. In figure 4 we present the different layers in the society in the left column, then some analyzed impacts in the second column and a flow-chart to show how events relate to each other in the right column.

We analyzed what impact the incident had on the different layers and moreover used the flowchart to show how decisions were made and had impact on other layers - both in Belgacom and in other societal organizations.

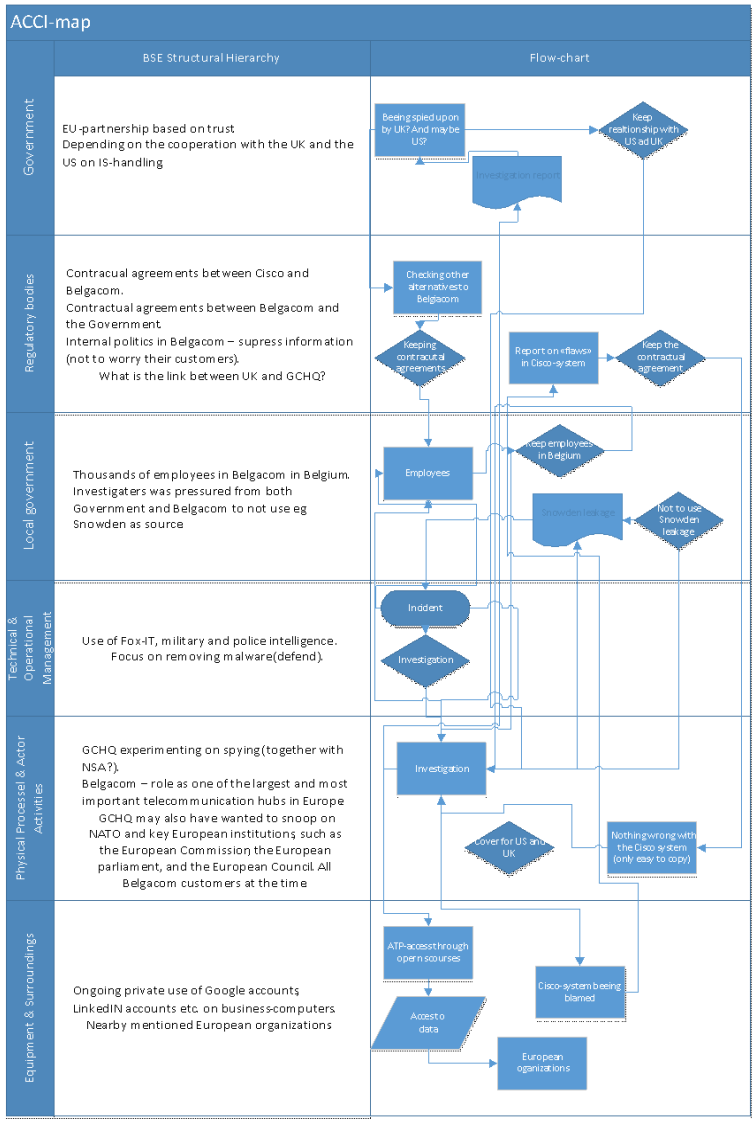



Figure 4: BSE Structural Hierarchy model analysis of Operation socialist

## 6 Current Conclusion

The socio-technical models appear useful in understanding and defining training scenarios as it gives us a good indication on both social and technical challenges from real life cases.

The **SBC Model** appears to be a good model for making scenarios for table top exercise regarding the Belgacom incident, since it helps to indicate were the organization is vulnerable from a strategic level within the organization. By using the SBC model, we can make exercise that show the relationship between different both technical and social functions within (in this case) Belgacom, and a scenario could be made to support this.

For **Kowalski's socio-technical model** we choose organizational and national level, but we think that for writing scenarios, we could have chosen both local government and other third-parties. We figured this model would be excellent for making scenarios for discussion exercises and table-top exercises. This model gives the instructors/trainers possibility to both focus and train the company and a third party. The idea of the model is though in a continual state of surface flux, it is also striving to reach a state of equilibrium or homeostasis (Kowalski, 1994). In our incident, this means that when we find the weakest link in the model, which might be the place to start modeling a scenario for exercise, by using this model, you may end up with different kind of scenarios and exercises.

The **BSE-model** with the flow-chart shows how well aligned the different events are between different levels in this hierarchy, and we also see a scenario involving all these levels. This model shows that all levels are connected and gives us the reason to believe that this model can be used for making scenarios for full-scaled exercises, but also be toned down and used for all other types of exercises.

When we analyzed the **Withword 8 criteria-model** we found that this is related to organizational level in first, and as the WOSP are made to follow up on strategic decisions, this model can be used for discussions exercises. This assumes Information Security as part of the WOSP's.

Below is a table outline the four different models and the type of exercise the actual incident can be applied.

Table 2: Using socio-technical models and real incident to build relevant scenarios for exercises

| Socio-technical model | Withford | SBC-model | Kowalski | BSE-model |
|---|---|---|---|---|
| Scenario | Operation Socialist | Operation Socialist | Operation Socialist | Operation Socialist |
| Appropriate for exercise | Discussion exercise | Table-top exercise | Discussion exercise<br>Table-top exercise<br>Simulation exercise | Full-scale exercise |

In figure 5 we map the different socio-technical models together with the scenarios for exercises mapped in figure 2, to attempt to visualize and compare. We may conclude

that by changing the models in one or another direction, they will be more suitable for the different kind of exercises. For example, the Kowalski model can float across the diagram based on the situation in the organization, and by that approach decide what exercise to consider.

We are proposing to name this comparing model a socio-technical system design framework for cyber security training exercises (STSD-CSTE).

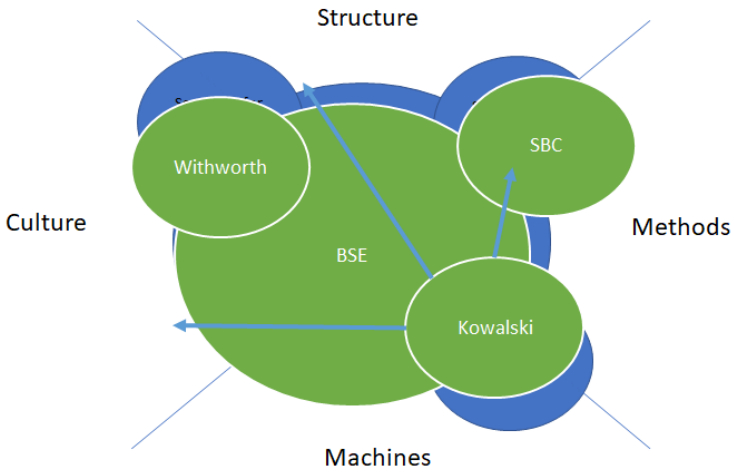



Figure 5: Framework for building relevant scenarios for exercises, based on socio-technical models to analyze real life incidents (STSD-CSTE)

## 7 Future Directions

Social-technical models enables us to introduce more holistic and near-to-life elements needed to be factored in designing scenarios. We need to verify and validate the findings we already have made, and to enhance and improve the STSD-CSTE model proposed. To validate the framework, we plan to test it when setting up exercises in the NCR environment. NCR will be an arena where testing, training, and exercise are tools to expose people, businesses, and units to realistic events and situations in a realistic but safe environment. The arena ensures efficient transfer of knowledge and building of real-world competence, that links together the strategic, operational, tactical and technical levels of decision making, by simulating the impacts of cyber security events on the levels of society, digital value chains and cyber infrastructure without harming the entities involved and their critical infrastructure.

In this paper we describe a root-cause analysis by using only four socio-technical models. In future work we will do a systematic-literature review of socio-technical

modeling in general and select the models that best meets when designing exercise and scenario in the Norwegian Cyber Range.

To ensure the best possible effect in the cyber-range arena in Norway, current existing information systems tools used in the community will be, for example, ISCMS (information security crises management systems) systems, and facilitate accurate comprehension of scenarios fitted the different systems. Additionally, there will be need of preparedness learning based on real life incidents.

When analyzing the outlined DSB's definitions of exercises, we found that there is no clear definition on cultural and machine exercises (lower left corner of our model). However, as mentioned there are examples of real-life incidents which has been used in teaching strategic and ethical exercises. We consider this as an area of which can be developed better in combining exercise-definitions and scenarios and have a work in progress in this matter.

As illustrated in figure 6, the more complex and capabilities involved in the training exercise, the more effort and resources must be put into planning.

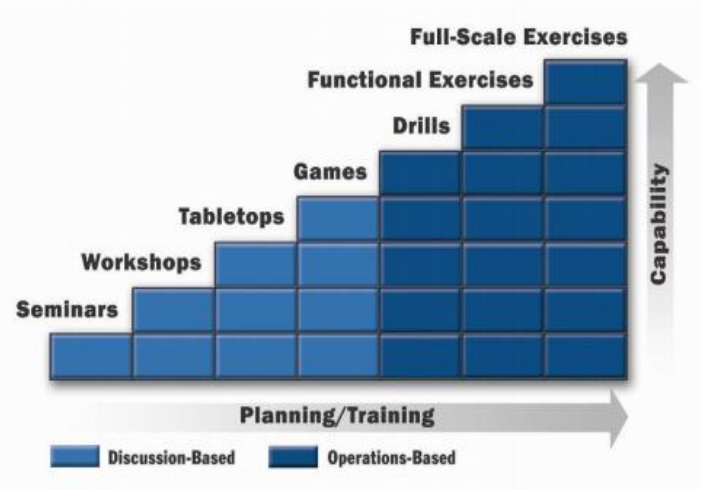



Figure 6: Exercise Types and Capacity Levels from (HSEEP, 2006)

Figure 6 also illustrates another adjacent topic; cost. A full-scale exercise requires far more resources than simple discussion meetings or tabletop exercises. By using a more granular (STSD-CTF) model, time and cost can be saved by facilitating management to help them identifying and choose appropriate test scenarios for the participating organization. By structured use of the (STSD-CTF) model scenario repository can be constructed. Scenario repository can be used to both re-use and exchange scenario and exercise. This may reduce costs of cyber security training and help to fill the existing competence gap for cyber security personnel in two ways: Directly to provide customized training exercise at low cost and secondly by allowing none security specialists to

participate in organizational learning exercises. Moreover, consequently distribute the knowledge to handle the cyber security problem across the organization.

Being a working in progress paper it is difficult to have clear conclusions yet. However as indicate in figure 1 there are 5 distinct steps in the design science research process, problem analysis step, solutions suggestion step, development step, evaluations step and conclusion. This paper has outlined a work in progress in step 1 and step 2. In the next step we will develop scenario exercises and refine the evaluation criteria to measure the effectiveness of these exercise to help deal with the problem of fill the gap between the demand and supply of cyber security specialist and cyber security trained users.

## 8 References

Carayon, P., Hancock, P., Leveson, N., Noy, I., Sznelwar, L., & van Hootegem, G. (2015). Advancing a sociotechnical systems approach to workplace safety – developing the conceptual framework. *Ergonomics*. https://doi.org/10.1080/00140139.2015.1015623

Carlsson, A., & Gustavsson, R. (2018). The art of war in the cyber world. In *2017 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2017 - Proceedings*. https://doi.org/10.1109/INFOCOMMST.2017.8246345

Cassano-Piché, A., Vicente, K. J., & Jamieson, G. A. (2006). *A SOCIOTECHNICAL SYSTEMS ANALYSIS OF THE BSE EPIDEMIC IN THE UK THROUGH CASE STUDY*.

Cisco. (2018). *Annual cyber security report*.

Computing Cases. (1983). Therac-25. Retrieved from https://computingcases.org/case_materials/therac/teaching_intro/Teaching_Intro.html

Dahlgren, M. A., & Öberg, G. (2001). *Questioning to learn and learning to question: Structure and function of problem-based learning scenarios in environmental science education*. *Higher Education* (Vol. 41).

DSB. (2016a). *Fullskalaøvelser*. Retrieved from https://www.dsb.no/globalassets/dokumenter/risiko-sarbarhet-og-beredskap/ovingsveileder/metodehefte_-fullskalaovelse.pdf

DSB. (2016b). *Funksjonsøvelser*. Retrieved from https://www.dsb.no/globalassets/dokumenter/risiko-sarbarhet-og-beredskap/ovingsveileder/metodehefte_funksjonsovelse.pdf

DSB. (2016c). *Metodehefte diskusjonsøvelse*. Retrieved from https://www.dsb.no/globalassets/dokumenter/risiko-sarbarhet-og-beredskap/ovingsveileder/metodehefte_diskusjonsovelse.pdf

DSB. (2016d). *Spilløvelser*. Retrieved from https://www.dsb.no/veiledere-handboker-og-informasjonsmateriell/metodehefte-spillovelse/

Gallagher, R. (2018, February 17). How U.K. spies hacked a European ally and got

away with it. *The Intercept_*. Retrieved from https://theintercept.com/2018/02/17/gchq-belgacom-investigation-europe-hack/

Idé, T., Lozano, A. C., Abe, N., & Liu, Y. (2013). Proximity-Based Anomaly Detection using Sparse Structure Learning. https://doi.org/10.1137/1.9781611972795.9

Karokola, G. R. (2012). *A framework for Securing a-Government Services, The case of Tanzania*. Stockholm University.

Kowalski, S. (1994). *IT Insecurity: A Multi-disiplinary Inquiry*. Stockholm University.

Kuechler, W., & Vaishnavi, V. (2012). *A Framework for Theory Development in Design Science Research: Multiple Perspectives*. *Journal of the Association for Information Systems* (Vol. 13).

Lalonde, C. (2007). *Proceedings of OLKC 2007-"Learning Fusion" CRISIS MANAGEMENT AND ORGANIZATIONAL DEVELOPMENT: TOWARDS THE CONCEPTION OF A LEARNING MODEL IN CRISIS MANAGEMENT*.

Li, F., Lai, A., & Ddl, D. (2011). Evidence of advanced persistent threat: A case study of malware for political espionage. In *Proceedings of the 2011 6th International Conference on Malicious and Unwanted Software, Malware 2011*. https://doi.org/10.1109/MALWARE.2011.6112333

Marquis-Boire, M., Guarnieri, C., & Gallagher, R. (2014, November 24). Secret Malware in European Union Attack Liked to U.S. and British Intelligence. Retrieved from https://theintercept.com/2014/11/24/secret-regin-malware-belgacom-nsa-gchq/

NSM. (2018). *Et sikkert digitalt Norge-IKT-risikobilde 2018*.

Oppland Arbeiderblad. (2017). Øvelse på kritsk dataangrep. Retrieved from https://www.oa.no/fylkesmannen/beredskap/oppland/ovelse-pa-kritisk-dataangrep/s/5-35-545812

Pelletier, L. G., Guertin, C., Paige Pope, J., & Rocchi, M. (2016). Homeostasis balance, homeostasis imbalance or distinct motivational processes? Comments on marks (2015) 'homeostatic theory of obesity.' *Health Psychology Open*, *3*(1). https://doi.org/10.1177/2055102915624512

Rahman, S., Momtazpour, M., Zhang, J., Sharma, R., & Ramakrishnan, N. (2015). Analyzing Invariants in Cyber-Physical Systems using Latent Factor Regression. https://doi.org/10.1145/2783258.2788605

Schoemaker, P. J. H., & van der Heijden, C. A. J. M. (2008). Integrating scenarios into strategic planning at Royal Dutch/Shell. *Planning Review*. https://doi.org/10.1108/eb054360

Telenor. (2018). *Digital Sterkere sammen*.

Whitworth, B., & Zaic, M. (2018). The WOSP Model: Balanced Information System Design and Evaluation. *Communications of the Association for Information Systems*. https://doi.org/10.17705/1cais.01217

Appendix 1
Hendelseshåndtering ved cyber-angrepet mot Østre Toten kommune
https://www.ototen.no/aktuelt/rapport-etter-dataangrepet.15279.aspx

Rapport

Grethe Østby, Stewart James Kowalski

# Hendelseshåndtering ved cyber-angrepet mot Østre Toten kommune

## Hva kan vi lære fra håndteringen?

28.09.2022

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for informasjonssikkerhet og kommunikasjonsteknologi


NTNU
Kunnskap for en bedre verden

# Historikk

**VERSJON**
1.0

**FORFATTER(E)**
Grethe Østby, Stewart James Kowalski

**OPPDRAGSGIVER(E)**
Østre Toten kommune

**OPPDRAGSGIVER REF.**
Kommunedirektør Ole Magnus Stensrud

**DATO**
28.09.2022

**ANTALL SIDER OG VEDLEGG**
24 sider, 3 vedlegg

# Innholdsfortegnelse


**Sammendrag. Det skjedde – hvordan ble det håndtert? 4**

**Introduksjon og bakgrunn 6**

**Metode 10**

**Vurdering av resultatene (diskusjon) 14**
*Cyber-angrep som egen risiko og sårbarhetsvurdering 14*
*IKT-hendelseshåndterings- og gjenopprettingsteam 16*
*Varslingsteam sensitive personopplysninger på avveie 18*
*Intern kommunikasjon – brudd i kriselinje (?) 18*
*Trening og øving 19*
*Krysskoordinering 22*

**Kort oppsummering og fremtidige vurderinger 22**

**Referanser 23**

**Vedlegg 1 - Mandat 25**
*Kriseledelsen gir oppdrag til en evalueringsgruppe 26*
*Avgrensing 27*
*Metode 27*
*Framdrift 27*

**Vedlegg 2 - Resultater 29**
*Spørreundersøkelsen 29*
Lærebokvurderinger av hendelseshåndteringen 31
Lovpålagte krav til samfunnssikkerhet og beredskap i kommunene 34
Sosio-teknisk tilnærming til hendelseshåndtering 35
Modenhetsundersøkelse (eksalering og de-eskalering av informasjon under hendelseshåndtering) 38
*Dybdeintervjuene 38*
Hvem var dine ulike kontaktpersonene i Østre Toten kommune (hvem ble det eskalert eller de-eskalerte informasjon til)? og Var du kontaktperson for noen utenom Østre Toten kommune (eksempelvis for etterforskning eller annet)? 47
Hva er det viktigste du lærte under hendelseshåndteringen? 52
Hva slags form for beredskapsplaner eller tiltakskort ble benyttet ift. ditt arbeid i krisehåndteringen? 56
Hvilke anbefalinger vil du gi til kommuner og andre organisasjoner? 57
Hvilke anbefalinger vil du gi til arbeidet med roller i krisehåndtering? 63
Hvilke anbefalinger vil du gi til arbeidet med opplæring, trening og øvelser? 66
Hadde du tenkt på noe før intervjuet som du tenkte det var viktig å fortelle meg for at man skal lære av hendelsen? 69

# Sammendrag. Det skjedde – hvordan ble det håndtert?

9. januar 2021 ble Østre Toten kommune utsatt for et cyber-angrep, et såkalt løsepengevirus. Omkring 240 virksomhets-systemer i kommunen ble utilgjengelige for bruk.

> «Løsepengevirus er en type skadevare som låser eller krypterer hele eller deler av innholdet på datamaskinen. Målet er å få brukeren til å betale løsepenger til angriperen. For at brukeren skal få tilgang til innholdet på egen datamaskin igjen, krever angriper at man betaler løsepenger, ofte i form av BitCoin.» [1]

Angrepet skjedde samtidig med håndteringen av den pågående covid19 pandemien, så organisasjonen var allerede under en krisehåndteringsdoktrine. Det ble allikevel tidlig lørdag morgen etter angrepet satt krisestab for å håndtere denne hendelsen spesielt, og prioriteringer ble gjort basert på forutsetningene som var til stede. Hendelseshåndteringen ble som kjent svært langvarig, og var en krevende prosess for organisasjonen.

I forbindelse med alle type hendelser som er av betydning, anmoder Statsforvalteren i det gitte området om å evaluere hendelser basert på sin instruks (forskrift) [2]. I Østre Toten sitt tilfelle ble det også tildelt skjønnsmidler fra Statsforvalteren, slik at ansatte skulle kunne frigjøres til å delta i evalueringen. Hovedmålene med evalueringen av cyber-sikkerhetshendelsen i Østre Toten var å både lære internt i kommunen av det som har vært erfart, men også at andre skal kunne lære av hendelsen. Rammene for evalueringen av cybersikkerhetshendelsen skulle utøves i en slik form at erfaringer og tilegnet kunnskap også skal kunne benyttes i undervisning, trening og øvelser. Dermed ble vi ved Norges Tekniskvitenskapelige Universitet (NTNU), Institutt for Informasjonssikkerhet og kommunikasjonsteknologi, som forsker på denne type hendelseshåndtering, plukket ut til å gjennomføre denne evalueringen. Mandatet er i sin helhet gjengitt i vedlegg 1.

Vi tilnærmet oss oppdraget med å gjennomføre en spørreundersøkelse, samt gjennomføre dybdeintervjuer. Av totalt n=38 som aksepterte å delta i forskningsprosjektet, svarte x=28 på hele spørreundersøkelsen og y=9 deltok i dybdeintervjuer. Resultater fra spørreundersøkelsen og dybdeintervjuene er presentert i vedlegg 2.

Arbeidet har gitt oss mye informasjon som kan benyttes til både opplæring, trening og øvelser, men vi vil allikevel trekke frem noen hovedfunn, som er spesielt viktige for kommunen selv, samt andre kommuner og organisasjoner som bør forberede seg på et cyber-angrep:

1) Cyber-angrep krever en egen plass på organisasjonens risiko- og sårbarhetsliste (kan ikke betraktes som strømbrudd eller ekom-feil).
2) Eksterne informasjonskrav er ekstraordinære, annerledes og mer krevende enn i en «normal» hendelse (f.eks. fra nasjonale sikkerhetsorganisasjoner, etterretningsorganisasjoner, CSIRT, databeskyttelsesmyndighet etc.).
3) Beredskapsplaner må inneholde en plan for og kontrakt med et eksternt IKT-hendelseshåndterings- og gjenopprettingsteam (hvis slikt personell ikke er en del av organisasjonen).
4) I tillegg bør også beredskapsplaner inneholde en plan for hvordan man håndterer sensitive personopplysninger på avveie.

5) Intern kommunikasjon omkring prioritering og løpende oppfølging av uløste situasjoner er svært krevende, og over tid kan krisestyringslinjen kortsluttes, og man trenger da en god plan for hvordan man ønsker å håndtere dette.
6) Vi anbefaler at det stilles krav om trening og øving av cyber-angrep på lik linje med andre hendelser, og det bør stilles krav til offentlige beredskapsorganisasjoner om å gjennomføre denne type øvelser i nær framtid.
7) Krysskoordinering (regulert) fra lokal koordinering (Statsforvalter) og nasjonale myndigheter (Nasjonal sikkerhetsmyndighet) i slike angrep skaper til tider forvirring og usikkerhet, og det må under dagens regime planlegges for å kunne håndtere begge deler.

I tillegg har vi funnet sammenhenger mellom de ulike tilnærmingene vi hadde i spørreundersøkelsen, samt gjort nye erfaringer ved bruk av modenhetsanalyse (da i dette tilfellet fordi vi benyttet den i etterkant av hendelsen, samt at den ble distribuert blant alle som deltok i spørreundersøkelsen i motsetning til å bli benyttet for å forberede for øvelser som vi tidligere har gjort). Resultatene fra dette vil bli presentert i vitenskapelige artikler, samt i Østby sin doktorgradsavhandling. Vi kan i denne sammenheng påpeke at det eksempelvis er for få svar på noen av spørsmålene i spørreundersøkelsen, og at disse dermed ikke kan benyttes i vitenskapelig sammenheng. Dette og andre forhold som har påvirkning på resultatene vil bli presisert i det øvrige vitenskapelige arbeidet. Svarene er imidlertid presentert i sin helhet i vedlegget i denne rapporten, for å gi en oversikt over hva undersøkelsen innebar.

En del av titlene i rapporten er ikke titler som eksisterer til vanlig, men er brukt for å gi et bilde av hva ansvaret besto i hendelseshåndteringen. Et slikt eksempel er gjenopprettingsansvarlig. Det var jo også slik at det i svarene i dybdeintervjuene ble benyttet navn, og disse navnene er da erstattet med titlene som er presentert under Vurdering av resultatene.

En kommune er en kompleks organisasjon med mange sektorer, og man skulle nok kanskje ønsket seg å gjøre flere dybdeintervjuer opp mot flere av sektorene, men vi valgte å plukke ut noen fra de ulike nivåene i organisasjonen. Dermed kunne vi vurdere tidligere akademisk arbeid på området, samtidig som vi har gitt noen muligheter til å vurdere hva disse resultatene kan bety for kommunen selv og andre kommuner og organisasjoner. Det bør være mulig å bygge opp gode scenarioer for øvelser ved å lese erfaringene fra deltakerne i dybdeintervjuene. Samtidig vil det altså være noe mangelfullt for enkelte sektorer og organisasjoner, men vi anmoder om å bruke materiellet i form av «hva ville i så tilfellet ha skjedd hos oss».

## Introduksjon og bakgrunn

Stadig flere organisasjoner også i Norge blir utsatt for målrettede cyber-angrep [3]–[6], og kunnskap om og forståelse for hvordan man skal håndtere slike hendelser er etterspurt [7], [8]. Tidligere studier har vist at det er behov for sosio-teknisk tilnærming til denne type hendelseshåndtering [9]–[11], og i sin avhandling [9] beskriver Kowalski hvordan man i en håndtering av cyber-sikkerhet kontinuerlig må ha fokus på både sosiale og tekniske forhold i en organisasjon. Dette er presentert i figur 1.

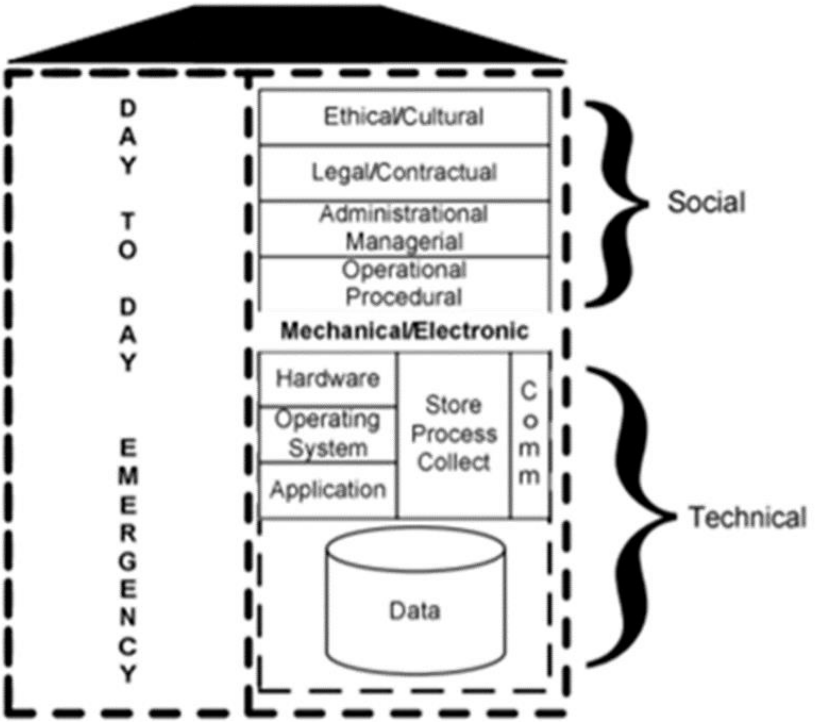



**Fig. 1.** Sosio-teknisk håndtering av cyber-hendelser [9]

Et nylig studie [10] foreslår også å kombinere denne type sosio-teknisk håndtering med National Institute of Standards and Technology (NIST) sitt rammeverk for hendelseshåndtering [12]. NIST sitt rammeverk er presentert i figur 2.

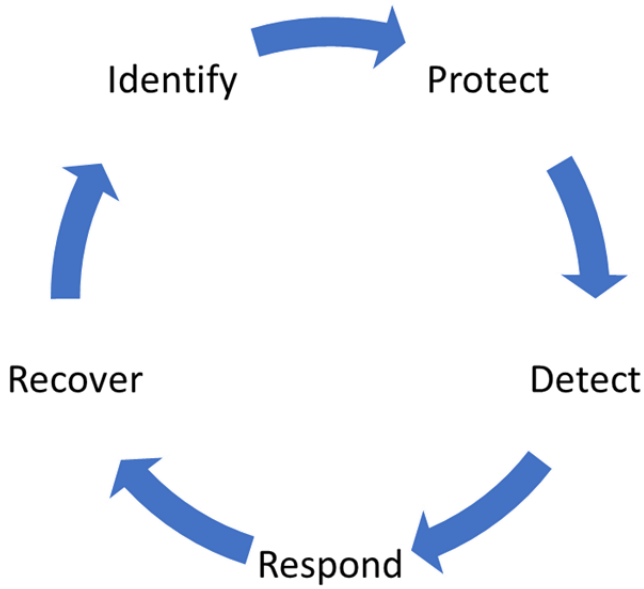



**Fig. 2.** NIST rammeverk for cyber-sikkerhet [12]

Tilsvarende rammeverk er foreslått i Nasjonal sikkerhetsmyndighet (NSM) sine grunnprinsipper for IKT-sikkerhet, som i stor grad likner NIST sitt rammeverk. Dette er presentert i figur 3.

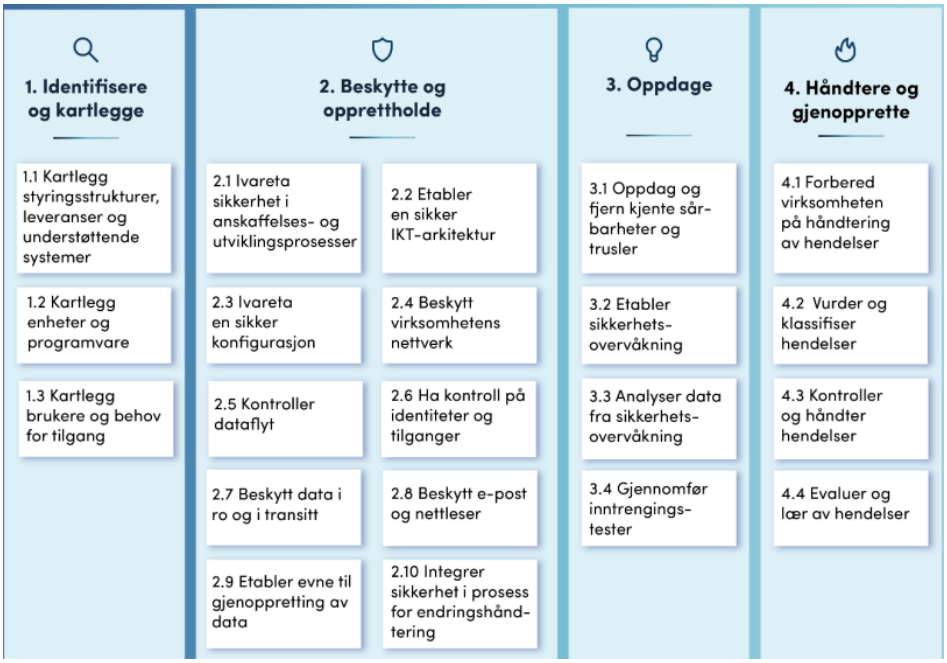



**Fig. 3.** NSM sine grunnprinsipper for IKT sikkerhet [13]

Den senere tid har også Nasjonal Sikkerhetsmyndighet (NSM) utarbeidet rammeverk for håndtering av cyberangrep [13], mens Næringslivets sikkerhetsråd (NSR) har gitt ut en Nødplakat for digitale angrep i samarbeid med NSM og Politiet [14]. Som beskrevet i NSM sitt rammeverk, er relevante lover og forskrifter i denne sammenheng blant andre Lov om forebyggende sikkerhet (sikkerhetsloven) med forskrifter, Lov om behandling av personopplysninger (personopplysningsloven) med forskrift, Lov om elektronisk kommunikasjon (ekom-loven), Straffeloven, Politiregisterloven, Lov om helseregistre og behandling av helseopplysninger (helseregisterloven), Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven), Lov om arkiv (arkivloven), Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven), Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) og Forskrift om offentlige arkiv (arkivforskrifta). I tillegg tillegges NSM ansvar for å koordinere IKT-sikkerhetshendelser ved angrep mot kritisk infrastruktur. Allikevel presiseres det i rammeverket til NSM at rammeverket ikke gjelder konsekvenshåndteringen av hendelsen. Det vil med andre ord være organisasjonen selv som må lage planer for håndteringen.

I Norge er det gitt et rammeverk for krisehåndtering for kommuner spesielt gjennom Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret [15] med dertil forskrift [16] og veiledning til forskriften [17]. Samtidig har Statsforvalteren et ansvar for å koordinere større hendelser i sitt geografiske område, og dermed på tross av nasjonal koordinering av IKT-hendelsen, skal altså Statsforvalteren koordinere konsekvensene av hendelsen. Det har derfor vært viktig i arbeidet med denne rapporten å også se på hvordan en kommune (eller en hvilken som helst annen organisasjon) vil måtte forholde seg til dette, og dermed også vurdere sine beredskapsplaner for å både kunne bli koordinert av nasjonale myndigheter samtidig som også av Statsforvalter. I tillegg har det blitt vurdert ulike andre interessenter som kommune-CSIRT, Kommunesektorens interesseorganisasjon (KS), Datatilsynet, og i Østre Toten sitt tilfelle også henvendelse fra Cyber-Forsvaret, som har måttet bli håndtert etter beste evne og etter kommunens besluttede intensjon om åpenhet rundt det som hadde skjedd.

Det å kunne lære fra kriser, eller det vi kan kalle kriseindusert læring, er en sjelden tilstand da en krise er en sjelden tilstand i seg selv [18]. Å lære fra øvelser på samme måte som læring fra hendelser er imidlertid anerkjent [19], og faktorer som støtter læringsaktiviteter i en øvelse kan betraktes som en teknikk som brukes i kunnskapsledelse.

> "Kunnskapsledelse er et sett med teknikker og praksiser som letter flyten av kunnskap inn i og innenfor firmaet." [20]

Overlappingen mellom kunnskapsledelse og organisatorisk læring gjør det imidlertid vanskelig å skille mellom de to [21], men man må anta at den organisatoriske læringen kan foregå uten ledelse. Organisatorisk læring har vært diskutert siden slutten av 1950-tallet [22], men vi vil argumentere for at øvelser også kan etablere grunnlaget for organisasjonslæring, spesielt for å forbedre kunnskap om informasjons- og cybersikkerhet.

> "Organisasjoner er gjenstander designet for menneskelige formål. Organisasjonens effektivitet avhenger av deres kontinuerlige redesign som

> svar på endrede verdier og en skiftende kontekst for handling. Organisatorisk læring vil da referere til denne prosessen med å kontinuerlig redesigne.» [23]

Beslutninger i en krise i beredskapsorganisasjoner tas ofte ved triage-beslutninger. "Selv om de er utviklet for enkeltpersoner, kan konseptene som brukes i et triagevurderingssystem også brukes på organisasjoner i krise" [24]. Innenfor informasjonssikkerhet viser eksempler at triage også kan være en del av hendelsesresponssystemene [25], og vi mener at dette er overførbart til både krisehåndtering og beslutningsteorier, og kan gjøre det lettere å trene sammen og lære av hverandre.

> "Beslutningstaking under usikkerhet handler om å ta valg hvis konsekvenser ikke er helt forutsigbare, fordi hendelser vil skje i fremtiden som vil påvirke konsekvensene av handlinger som tas nå." [26]

Vi mener at øvelser ikke bare kan bidra til teamlæring [27], men også til å legge grunnlaget for organisatoriske beslutninger for endringer for å forbedre modenhet innenfor informasjonssikkerhet og dessuten håndtere fremtidige kriser som har samme mengde usikkerhet.

For å kunne få til en slik læring i øvelser, skal det allikevel til en planlegging av slike øvelser, blant annet med bakgrunn i nettopp tidligere hendelser [11], men også 1) sårbarhetsvurderinger i den gitte organisasjonen, 2) vurdering av historiske trusler og angrep, 3) modenhetsundersøkelser, 4) tilrettelegging for gode leksjoner, og 5) spesifikke sosio-tekniske læringsartifakter i løpet av øvelsene [28]. For å nå målet i mandatet om at både Østre Toten og andre organisasjoner skal lære av hendelsen, ble dermed spørsmål omkring disse forholdene inkorporert i spørreundersøkelsen, men også som åpne spørsmål i dybdeintervjuene.

Siste del av spørreundersøkelsen var en ren modenhetsundersøkelse utviklet av Wahlgren og Kowalski [29], som er rettet mot evnen til å gjennomføre hendelseshåndtering dersom en IKT-sikkerhetshendelse skulle oppstå.

> «En prosess i en modenhetsmodell kan vurderes i mer enn ett prosjekt (dvs. flere forekomster av en prosess). Alle forekomster er samlet for å vurdere prosessen. Økning av antall prosessinstanser i vurdering bør derfor ikke tolkes som en måling av organisatorisk omfang.» [29]

Som vist i figur 4, består Wahlgren og Kowalski modenhetsmodell av en matrise hvis rader representerer ulike modenhetsnivåer og hvis kolonner representerer ulike modenhetsattributter. De brukte ISACAs[1] [30] modenhetsmodell som grunnlag for sin modell. Modenhetsnivåene er de samme som de fem modenhetsnivåene Humphrey et al. benyttet [31], og i likhet med ISACA la Wahlgren og Kowalski til et sjette nivå "Ikke-eksisterende". De brukte ISACAs modenhetsattributter som utgangspunkt, men tilpasset dem rundt eskalering av IT-relaterte sikkerhetshendelser.

[1] ISACA var tidligere kjent som Information Systems Audit and Control Association, men bærer nå kun navnet i form av akronymet ISACA

| Attribute / Level | 1 Awareness | 2 Responsibility | 3 Reporting | 4 Policies and standards | 5 Knowledge and education | 6 Procedures and tools |
|---|---|---|---|---|---|---|
| 0 Non-existent | | | | | | |
| 1 Initial | | | | | | |
| 2 Repeatable | | | | | | |
| 3 Defined | | | | | | |
| 4 Managed | | | | | | |
| 5 Optimized | | | | | | |

**Fig. 4.** Modenhetsmodell [29]

> «Det er åtte forskjellige modenhetsattributter i Wahlgren & Kowalski sin modell:
> A. Bevissthet omhandler ulike aspekter av hvor bevisste ansatte er på ulike IT-relaterte sikkerhetshendelser.
> B. Ansvar omhandler fordeling av ansvar innen organisasjonen for IT-relaterte sikkerhetshendelser.
> C. Rapportering omhandler rapporteringskanalene og hvordan regelmessig rapportering av IT-relaterte sikkerhetshendelser gjøres.
> D. Retningslinjer omhandler ulike retningslinjer for IT-relaterte sikkerhetshendelser.
> E. Kunnskap omhandler ulike ferdigheter og kunnskaper som trengs for å håndtere IT-relaterte sikkerhetshendelser.
> F. Prosedyrer omhandler ulike prosedyrer for håndtering av IT-relaterte sikkerhetshendelser.
> G. Midler omhandler ulike verktøy for håndtering av IT-relaterte sikkerhetshendelser.
> H. Struktur omhandler ulike forhåndsdefinerte grupper for håndtering av IT-relaterte sikkerhetshendelser.» [29]

Dette er første gang denne modellen er testet hos en organisasjon i etterkant av en hendelse, og må omtales deretter uten sammenlikning med andre undersøkelser. Som nevnt i sammendraget så vil resultatene fra dette arbeidet presenteres i vitenskapelige artikler og Østby sin doktorgradsavhandling.

I det følgende presenteres valgt metode for arbeidet, vurdering av resultatene (diskusjon) og en kort oppsummering med fremtidige vurderinger av nødvendig arbeid. Mandatet og deler av resultatene fra spørreundersøkelsen og dybdeintervjuene presenteres i henholdsvis vedlegg 1 og vedlegg 2.

## Metode

I dette arbeidet har vi benyttet oss av forskningsmetodikken «Designvitenskapelig forskning innenfor informasjons systemer» (DSRIS) som har vist seg nyttig når man skal utvikle og teste nye artefakter innenfor informatikk [32]. Designvitenskapelig forskning innenfor informasjons systemer (DSRIS) er en metodikk som kan utføres for å "teste innovasjoner og ideer som kreerer resultater gjennom utviklingsprosessen av artefakter på en effektiv og samtidig nyttig måte" [32].

Hvordan man jobber med DSRIS er presentert i en oppgave skrevet av G. R. Karokola [33]. Han visualiserte denne tilnærmingen som skissert i figur 5. Imidlertid har vi modifisert Karokola sin modell, og da vi allerede tidligere har foreslått løsninger (induktiv tilnærming) slik som beskrevet i mandatet, så har dette altså vært det første steget i prosessen i vårt tidligere arbeid, i stedet for abduktiv tilnærming som Karokola benyttet.

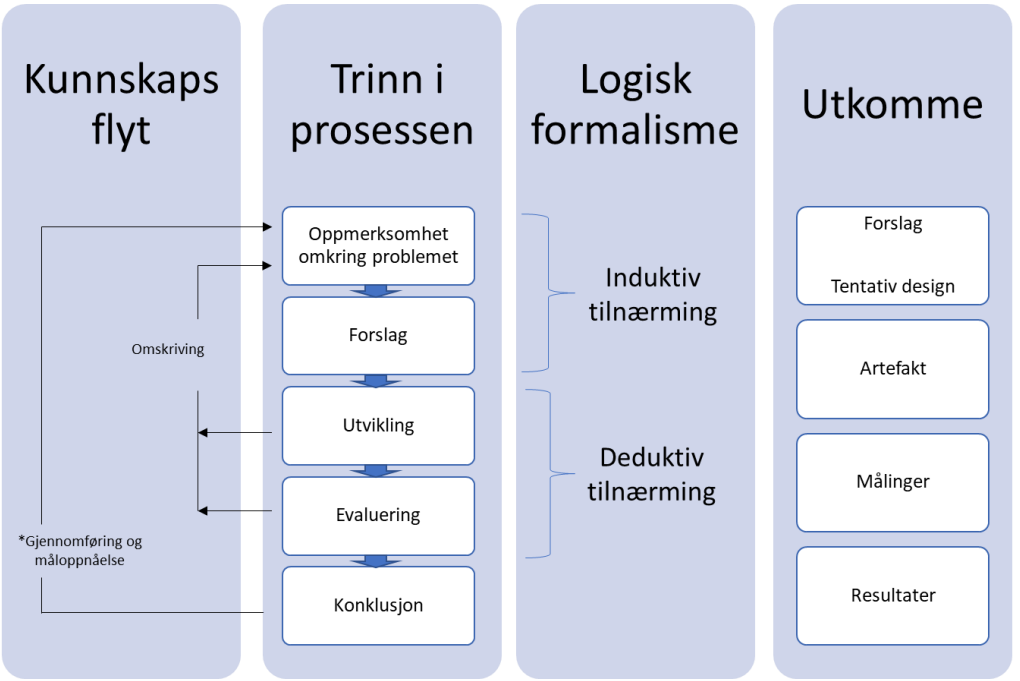



**Fig. 5.** Designvitenskapelig forskning innenfor informasjons systemer – modifisert [33]

Da forskningsarbeidet i Østre Toten kommune også skal benyttes i Østby sitt totale PhD-arbeid, så ble arbeidet i stor grad lagt opp til å verifisere tidligere arbeid. Som visualisert har Østby tilnærmet seg sitt PhD-arbeid med det som kan omtales som en induktiv tilnærming (i stedet for abduktiv eller deduktiv). Induktiv tilnærmingen starter med å først observere et fenomen og deretter generalisere om fenomenet som fører til teorier som kan falsifiseres eller valideres [9]. Vi presenterte problemstillingen for Østre Toten kommune gjennom en tidligere analyse av en preventiv beslutning i Gjøvik kommune, hvor vi den gang benyttet SBC-modellen i en sosioteknisk kontekst (se figur 1) kombinert med NIST sitt krisehåndteringsrammeverk (se figur 2) for å presentere informasjon og forslag til fremdrift i Østre Toten kommune. Vårt foreslåtte kombinasjonsrammeverk er presentert i figur 6.

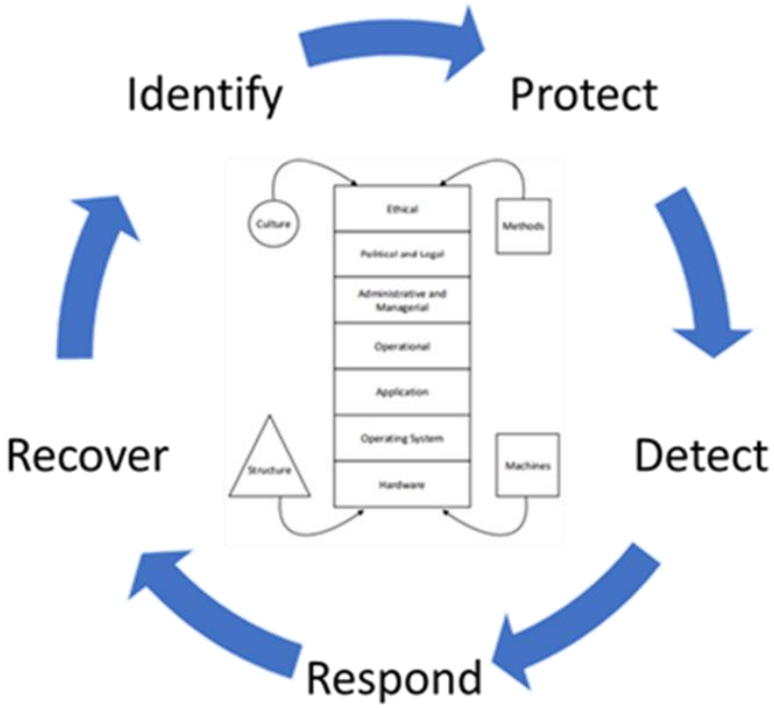



**Fig. 6.** Et sosio-teknisk og risiko-ledelses rotårsaksanalyse rammeverk [10]

Dette var dermed utgangspunktet for en deduktiv tilnærming i Østre Toten kommune, hvor spørreundersøkelsen var lagt opp til å undersøke hendelseshåndteringen ved å benytte disse rotårsaksmodellene i kombinasjon, samtidig som det ble gjennomført spørsmål knyttet opp mot krav i lovverk og nasjonale forskrifter og veiledere for beredskap [15], [16], [34], og avslutningsvis en modenhetsundersøkelse [29]. Noen av disse spørsmålene er overlappende, og trigget dermed spørsmål fra noen av deltakerne om dette. Fra vårt perspektiv har det vært viktig å nettopp se hvordan man kan kombinere ulike rammeverk (eksempelvis NIST [12], sosio-tekniske rammeverk [9], lovverk [15]), hva som i så tilfelle er overlappende, og hva som mangler i de ulike rammeverkene. De forskningsmessige resultatene fra dette vil som nevnt bli presentert i vitenskapelige artikler, samt i Østby sin doktorgradsavhandling samstemt med tidligere arbeid.

I tillegg til spørreundersøkelsen, så ble det gjennomført 9 dybdeintervjuer. Målsettingen med dybdeintervjuene var å få et bedre innblikk i læring i organisasjonen [18], [20], [21], [22], [23] som også andre kan lære av. Disse ble gjennomført i en semistrukturert form, med temaene 1) type involvering i hendelseshåndteringen, 2) kontaktpersoner i Østre-Toten kommune med fokus på eskalering og de-eskalering, 3) kontaktpersoner utenfor Østre-Toten, 4) hovedoppgaver i hendelseshåndteringen, 5) læring fra hendelsen, 6) anbefalinger til andre kommuner og andre organisasjoner, 7) anbefalinger til arbeidet med trening og øvelser, 8) roller i krisehåndtering av denne type kriser, og avslutningsvis 9) om det var tanker respondenten hadde forberedt og ønsket å formidle.

Utvalget av respondenter ble valgt med bakgrunn i tidligere arbeid i Østby sitt stipendiatprosjekt, for å få en oversikt over krisehåndteringen både på strategisk, taktisk og operativt nivå, og for dermed å kunne møte den deduktive tilnærmingen til dette arbeidet i form av utvikling og evaluering. Østby sitt tidligere arbeid er presentert i figur 7.

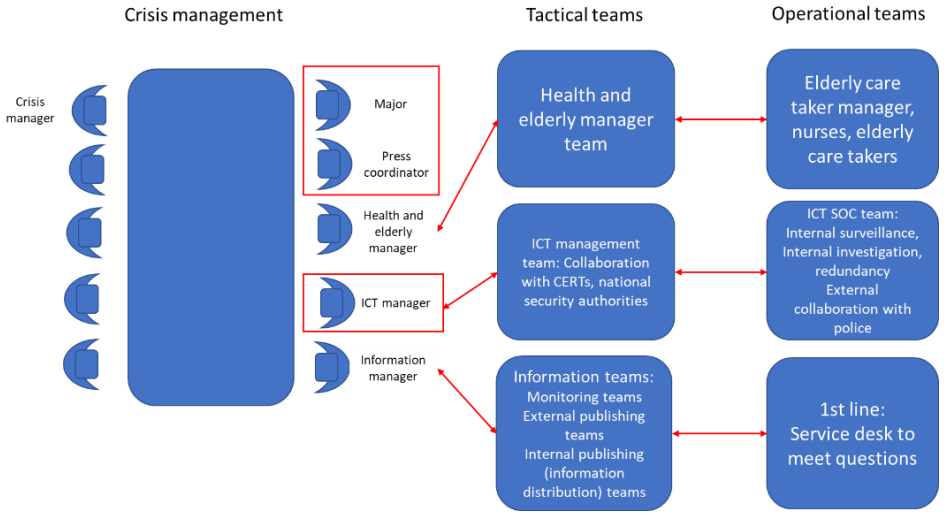



**Fig. 7.** Roller ved cyber-hendelser [35]

I tillegg ble det valgt respondenter fra utenfor organisasjonen for å vurdere informasjonsbehovet ut og inn av organisasjonen. Dette baserer seg også på Østby sitt arbeid fra samme artikkel [35], som er presentert i figur 8.

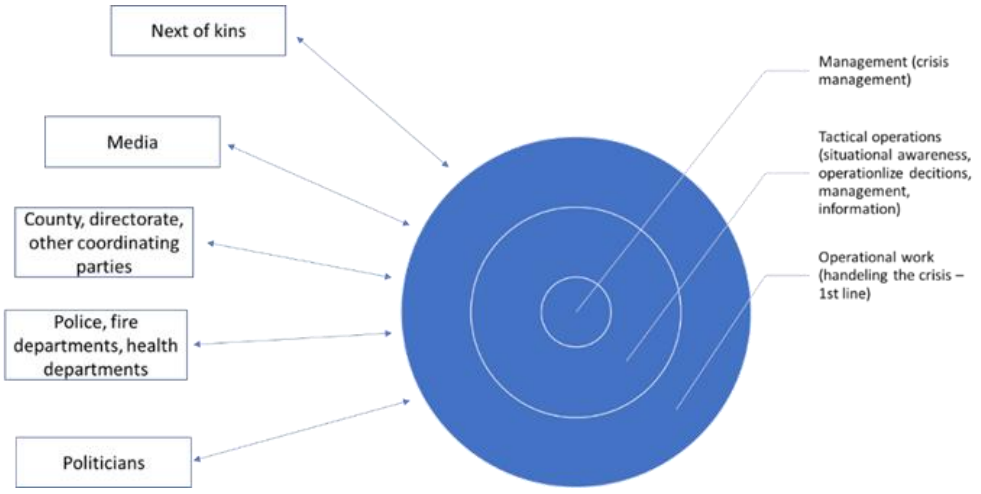



**Fig. 8.** Behov for informasjon i kriser [35]

Ved overgang fra vurdering av hendelseshåndteringen i seg selv, til dernest å vurdere hvordan man kan lære fra organisasjonen, ble det stilt åpne spørsmål i dybdeintervjuene, men også «naturlige» oppfølgingsspørsmål for å vurdere hvordan man kan bygge opp spillstab for øving [36] av de da endrede forutsetningene vi har sett.

# Vurdering av resultatene (diskusjon)

Hovedfunnene i undersøkelsen kan som nevnt i sammendraget deles inn i 7 områder:

1) Cyber-angrep krever en egen plass på organisasjonens risiko- og sårbarhetsliste (kan ikke betraktes som strømbrudd eller ekom-feil).
2) Eksterne informasjonskrav er ekstraordinære, annerledes og mer krevende enn i en «normal» hendelse (f.eks. fra nasjonale sikkerhetsorganisasjoner, etterretningsorganisasjoner, CSIRT, databeskyttelsesmyndighet etc.).
3) Beredskapsplaner må inneholde plan for og kontrakt med et eksternt IKT-hendelseshåndterings- og gjenopprettingsteam (hvis slikt personell ikke er en del av organisasjonen).
4) I tillegg bør også beredskapsplaner ha et kapittel om hvordan man håndterer sensitive personopplysninger på avveie.
5) Intern kommunikasjon omkring prioritering og løpende oppfølging av uløste situasjoner er svært krevende, og over tid kortsluttes krisestyringslinjen.
6) Det bør gjennomføres trening og øving av cyber-angrep på lik linje med andre hendelser, og vi anbefaler at det stilles krav til offentlige beredskapsorganisasjoner om å gjennomføre denne type øvelser i nær framtid.
7) Krysskoordinering (regulert) fra lokal koordinering (Statsforvalter) og nasjonale myndigheter (Nasjonal sikkerhetsmyndighet) i slike angrep skaper til tider forvirring og usikkerhet.

## Cyber-angrep som egen risiko og sårbarhetsvurdering

Det ble stilt spørsmål vedrørende gjennomføring av risiko og sårbarhetsvurdering både som en del av tekstbok-delen av undersøkelsen og også som en del av samfunnskravene (lover, forskrifter og veiledere) i undersøkelsen. Fra tekst-bok delen var det kun 4 som kjente til at det var gjort en risikovurdering av cyber-angrep før hendelsen, mens 24 svarte nei på dette. Av de 4 som kjente til at det var gjort en risikovurdering av cyber-angrep, svarte allikevel 1 at dette var utført på strategisk nivå, 1 at det var utført på taktisk nivå, mens 3 svarte at det var utført på operativt nivå. Fra samfunnskravsdelen og deri oppfølgingsspørsmål til de 12 som svarte ja om risiko- og sårbarhetsvurderingen ble gjennomgått ved siste revisjon av kommunedelplaner i henhold til Sivilbeskyttelsesloven §14, svarte 4 ja, 0 nei og 8 vet ikke. På spørsmål om cyber-angrep som hendelse var blitt vurdert i henhold til §14, svarte 1 ja, 4 nei og 7 vet ikke, og på spørsmål om cyber-angrep ble vurdert ved siste revisjon av kommunedelplaner svarte 1 ja, 3 nei, og 14 vet ikke. Det er altså 4 personer i begge delene av undersøkelsen som har hatt et forhold til risikovurderinger, og det kan synes som om at ja, det er gjennomført risikovurdering av cyber-angrep på operativt nivå, men at dette nødvendigvis ikke er knyttet opp mot lovhjemmelen med dertil oppfølging i revisjon av kommunedelplaner.

Hvorvidt en god helhetlig risiko-analyse av cyber-angrep ville medført et større fokus på tiltak og gode beredskapsplaner er jo uansett usikkert, spesielt med tanke på at man ikke før denne hendelsen hadde sett noe liknende med samme type konsekvenser i andre offentlige organisasjoner i Norge. Vi vet jo heller ikke om de 4 som har svart i begge delene av undersøkelsen her refererer til «modenhetsundersøkelsen» ATEA refererer til

(se vedlegg 2, side 44) eller risikovurderingen KPMG refererer til [37]. Sammenliknet med en sosio-teknisk tilnærming til risiko-vurdering, så dekker jo også en slik risikovurdering kun deler av hva som er anbefalt. Dette kan visualiseres som i figur 9.

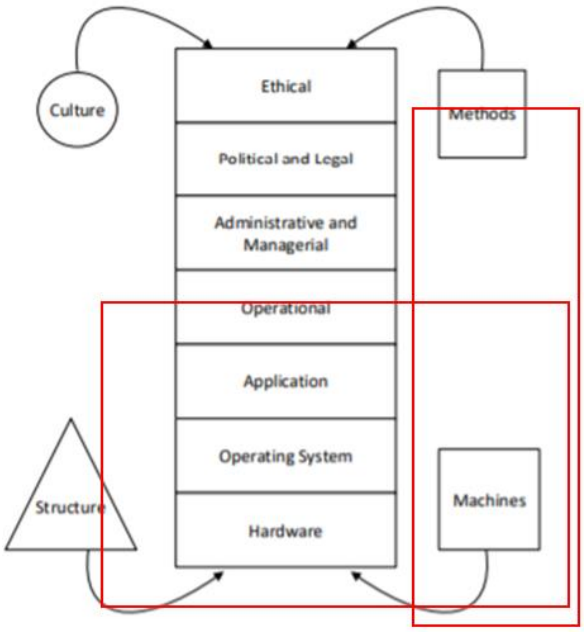



**Fig. 9.** Delvis risikoanalyse

Uansett så kan man basert på funnene si at det var liten kjennskap til risikovurdering av denne type hendelse. Konsekvensene av å ikke ha gjort en slik risikovurdering som både anbefales i tekstbøker for informasjonssikkerhet og er hjemlet ved nasjonale lover, forskrifter og veiledere har jo vært store, og som ordfører i kommunen peker på, så er det viktig også for folkevalgte å nå etterspørre rapporter på risikoarbeidet rundt cyber-angrep.

Informasjonskrav

Som nevnt i innledning- og bakgrunnskapittelet, så er informasjonsbehovet- og dertil trykk på organisasjonen noe annerledes enn i en vanlig hendelse. Dette kan presenteres ved en modifisert versjon av figur 8, her presentert i figur 10.

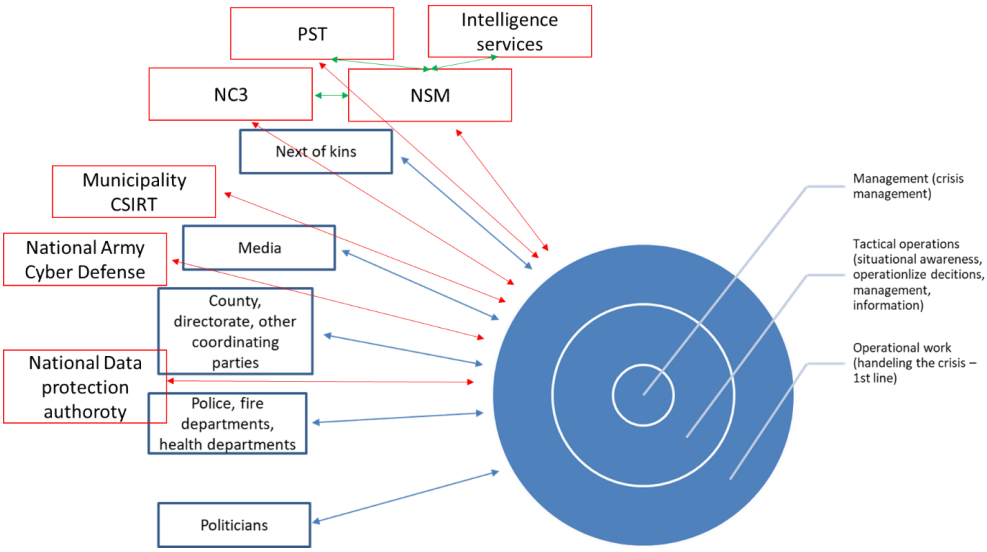



**Fig. 10.** Behov for informasjonsdeling ved cyber-angrep - modifisert [35]

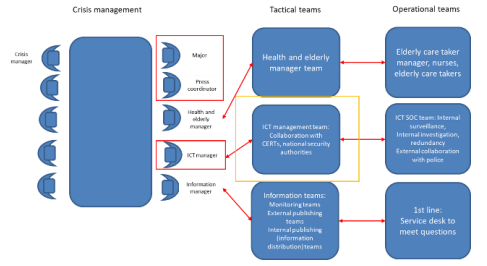
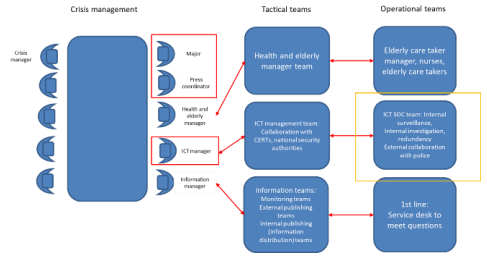
«Felles cyberkoordineringssenter (FCKS) består av NSM, Etterretningstjenesten, PST og Kripos (NC3), og ledes av NSM.» [13] Men selv om NSM har koordineringsansvaret, så var altså innsatsteamet i Østre Toten i dialog med flere av enhetene opptil flere ganger. I stor grad handlet dette om å gi fra seg informasjon, og lite falt tilbake til organisasjonen – før som kommunedirektøren nevner, at det måtte kreves å få innsyn i en rapport som var skrevet.

### IKT-hendelseshåndterings- og gjenopprettingsteam

Umiddelbart ble ATEA som er hovedsamarbeidspartner for IKT-sikkerhet i Gjøvik-regionen innhentet for å hjelpe til med gjennopprettingsarbeidet. Prioritering ble gjort basert på liv og helse, og arbeidet ble satt i gang med hjelp av teamet fra ATEA. Prioriteringen ble oppdatert noe i begynnelsen, men det kommer klart frem fra intervjuene at det er denne prioriteringen alle har måttet forholde seg til. Og gjennom tilfeldighetenes spill (?) ble det gjennom en god rådgiver/kontaktperson i KS foreslått navngitte personer i KPMG som også kunne hjelpe til og gi råd om selve ledelsen av hendelseshåndteringen, deri dialog med NC3, NSM og andre, samt det operative arbeidet som gjelder etterforskning og gjenoppretting.

Opp mot den opprinnelige modellen som Østby og Katt [35] har foreslått for organisering av hendelseshåndtering av cyber-sikkerhetshendelser, med et taktisk og et operativt team, er det ikke store avvik i forhold til type arbeid, men noen forhold ble gjort annerledes i hendelseshåndteringen i Østre Toten, samt at opplevelsen av om det var taktisk arbeid eller operativt arbeid var flytende. Selv om IT-sjef i utgangspunktet var alene i kriseledelsen, ble det så snart IKT-innsatsleder kom på plass (onsdag etter hendelsen), også til at vedkommende deltok i kriseledelsen. Det var også slik at både for det første kriseledelse ved kommunedirektør, og for det andre taktisk ledelse ved IKT-innsatsleder, og også de operative teamene var i kontakt med hhv. politi og NC3. IKT-innsatsleder var i starten leder for begge oppgaver, men hadde altså to forskjellige

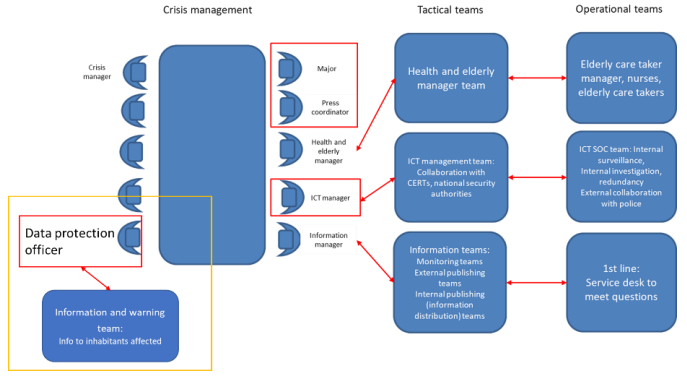
eksperter fra ATEA/KPMG til å støtte seg mot det ulike arbeidet i de to teamene. IKT-innsatsleder sluttet i sin stilling i Østre Toten i løpet av mai 2021.

| | |
|---|---|
| Taktisk team:<br><br>IKT-innsatsleder (frem til juni 2021)<br>Innleid ressurs fra Accenture (fra juni 2021)<br>Rådgiver fra KPMG<br>IT-sjef (ble borte fra teamet når han ble flyttet til IKOMM)<br>Økonomisjef |  |
| Operativ team:<br><br>Også IKT-innsatsleder (frem til juni 2021)<br>Gjenopprettingsansvarlig (fra juni 2021)<br>Sikkerhetseksperter fra først ATEA deretter KPMG<br>➔ Gjenopprettelseseksperter<br>➔ Etterretningseksperter |  |

Det som er viktig å få med seg, er at Østre Toten ikke var rustet med personell for å dekke dette arbeidet, hverken på taktisk eller operativt nivå. For Østre Toten og andre organisasjoner er det dermed viktig å kunne forberede for å få på plass slike team i en tilsvarende krise. Om disse er interne eller eksterne bør være opp til den enkelte organisasjon, men det bør gjøres avtaler og opprettes varslingslister/navnelister for beredskapsplanverket.

## Varslingsteam sensitive personopplysninger på avveie

Da hendelsen eskalerte med at sensitive personopplysninger ble lagt ut på det mørke nettet, ble også personvernombud hentet inn i kriseledelsen. For å håndtere informasjonsutveksling med berørte (evt. pårørende) ble det opprettet et varslingsteam:

| | |
|---|---|
| Varslingsteam<br><br>Personvernombud<br>En person fra voksenopplæringen<br>En person som tidligere hadde ledet psykososialt kriseteam i Østre Toten med helsefaglig bakgrunn<br>En kommunikasjonsrådgiver<br>Juridisk hjelp fra KPMG |  |

Man vet jo ikke nødvendigvis om dette er de eksakt rette personene for en annen organisasjon, men det bør allikevel ligge i beredskapsplanen en beskrivelse av oppgaver, samt en varslingsliste med nødvendige ressurser. Oppgavene som ble utført er godt beskrevet i resultatene fra intervju med personvernombud.

## Intern kommunikasjon – brudd i kriselinje (?)

Over tid viste det seg at kriselinjen med styring fra kriseledelsen skapte tretthet i organisasjonen. Dette gjaldt spesielt på taktisk nivå, hvor vi erfarer at skolesjef og økonomisjef beskriver dette på en god måte. Når det hadde gått en tid, og trettheten i organisasjonen oppsto fordi man ikke fikk løst oppgavene sine og fortsatt brukte private telefoner og annet for å løse oppdrag, mistet man i noen grad lojaliteten til krislinjene. Det ble derfor da en lettelse for eksempelvis skolen når man kunne ha direkte kontakt med gjenopprettingsansvarlig i det operative innsatsteamet. Den observante leser vil jo da ha sett at her ble det en form for brudd i krisehåndteringslinjen, samtidig som det ble høyere press på det operative IKT-innsatslederteamet (se figur 11). Men, dette ga samtidig en optimisme ute i organisasjonen. Det skal allikevel sies at det operative teamet under ledelse av gjenopprettingsansvarlig hadde klare føringer/prioriteringer fra kriseledelsen.

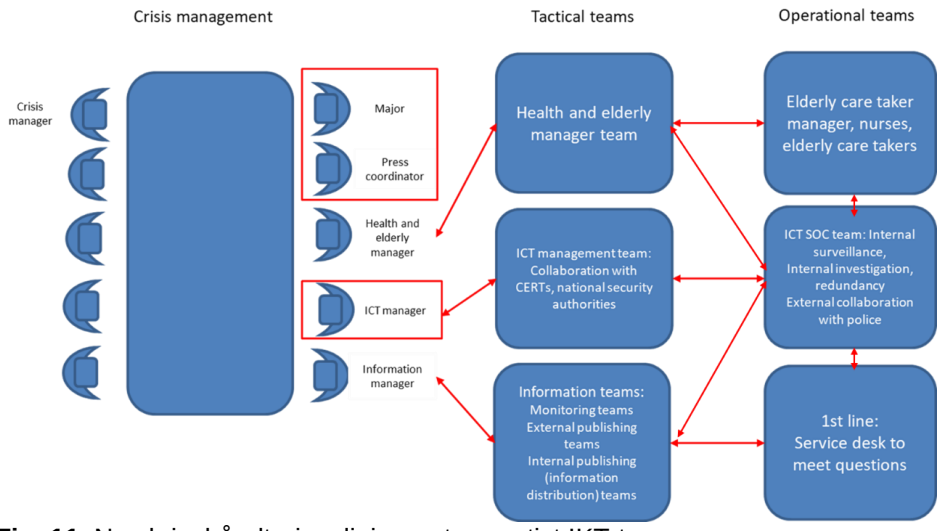



**Fig. 11.** Nye krisehåndteringslinjer mot operativt IKT-team

Hvorvidt dette er en god løsning må den enkelte organisasjon ta stilling til, og også vurdere ressurser i forhold til, men man bør vurdere presset på det operative IKT-teamet i hendelsesforløpet når dette på et tidspunkt skjer. I tillegg bør det da være enighet og tillit til at dette kan fungere godt for hele organisasjonen. Det som da også er viktig er at kontaktpersonene i gjenopprettingsteamet kjenner prioriteringen til ledelsen.

## Trening og øving

I spørreundersøkelsen kom det klart frem at de fleste ikke kjente til om organisasjonen hadde et sikkerhetsprogram. Et sikkerhetsprogram var beskrevet som at «det består av en organisasjonsplan med dertil oppgaver/funksjoner som det er behov for, sertifiseringsprogram, utdanning, trening, øvelser m.m.» Hele 25 svarte negativt på dette, mens 3 svarte positivt.

I intervjuene var det allikevel stor enighet om at slike hendelser må trenes og øves på. Under spørsmål om hva de hadde lært gjennom hendelsen, ble det allikevel gjerne litt stille, og det var ikke like enkelt å analysere hva organisasjonen har lært av hendelsen. Når det ble spurt litt mer konkret om beredskapsplaner, så kom det imidlertid tydeligere frem noen forhold, deri forståelsen av hva et cyber-angrep innebærer med dertil konsekvenser i organisasjonen som må håndteres.

Et eksempel er ved sykehjemmet, hvor de hadde planer for bortfall av strøm, og dermed hadde et døgn gammel liste med oversikt over pasienter og hvilke medisiner de enkelte skulle ha. Men, for å komme seg inn i medisinskapet skulle de egentlig benyttet en kortløsning, som da ikke lenger var aktivt. Andre systemer som var ute av drift var også varsling/alarm hos den enkelte beboer, noe som medførte at beboere måtte ta i bruk bjeller. Denne type eksempler vil være gjeldende også for andre organisasjoner, og kan enkelt skrives inn i scenarioer for øvelser [11].

I tillegg må man etter å ha vurdert hvilket modenhetsnivå den enkelte organisasjon er på sette opp trening og øvelser tilpasset nivået, for deretter å sette inn sosio-tekniske tiltak

for å dekke et skritt av gangen [38]. Dette kan visualiseres som en prosess, slik som presentert i figur 12.


**Fig. 12.** Modenhets forbedringsprosess [38]

Er modenheten generelt på et lavt nivå, så kan det være aktuelt å starte med enkle seminarer/opplæring eller diskusjonsøvelser, mens man ved et høyt modenhetsnivå gjerne kan arrangere funksjonsøvelser og fullskalaøvelser. Ulike type øvelser for slik trening er presentert i figur 13 [39], og det er også gode veiledere for øvelser hos Direktoratet for samfunnssikkerhet og beredskap (DSB) [40] og hos The European Union Agency for Cybersecurity (ENISA) [41].

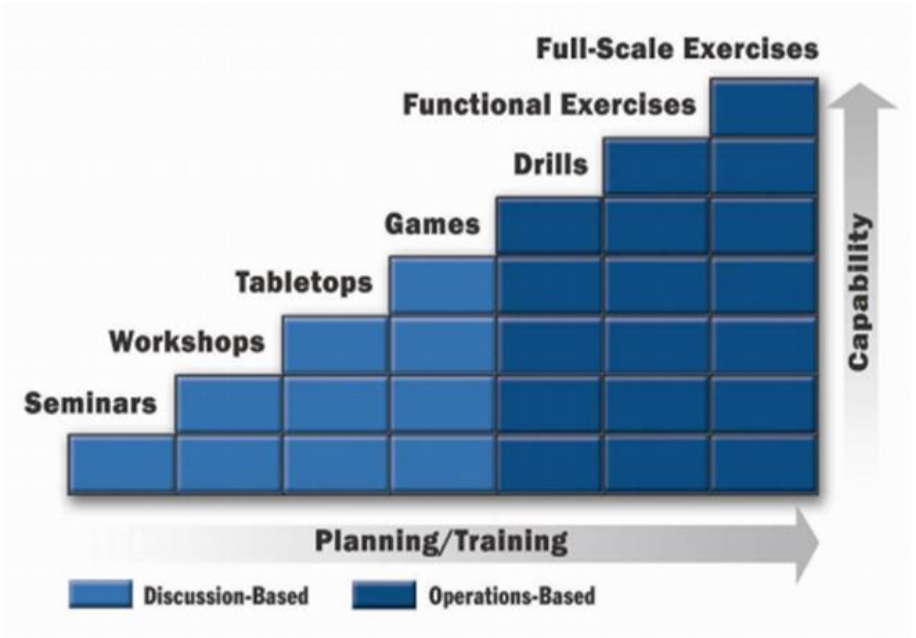



**Fig. 13.** Ulike type øvelser [39]

Det kan altså være lurt å starte på det laveste nivået dersom modenheten er lav, og vi anbefaler gjerne å starte med diskusjonsøvelser slik som presentert på ovelse.no. Dette er diskusjonsøvelser innenfor kjente temaer av informasjonssikkerhet, med noen gode diskusjonsspørsmål og gode råd. Disse øvelsene er planlagt for å ha en øvingsleder, med dertil egen informasjon til vedkommende, slik at det skal være mulig å forberede seg til øvelsene på en god måte.

Når det gjelder mer avanserte øvelser som funksjonsøvelser og fullskalaøvelser for organisasjoner, så anbefaler vi å forberede øvelser gjennom å skaffe seg god kunnskap om organisasjonen som skal øves [28], for deretter å lage et godt øvingsdirektiv med øvingsmål og scenario nettopp basert på nivået i organisasjonen. For gjennomføring av øvelsen foreslår vi å tilpasse en spillstab til den organisasjonen som skal øves, slik som presentert i figur 14 og figur 15, visualisert med farger i forhold til hvordan teamene bør bygges opp i spillstab.

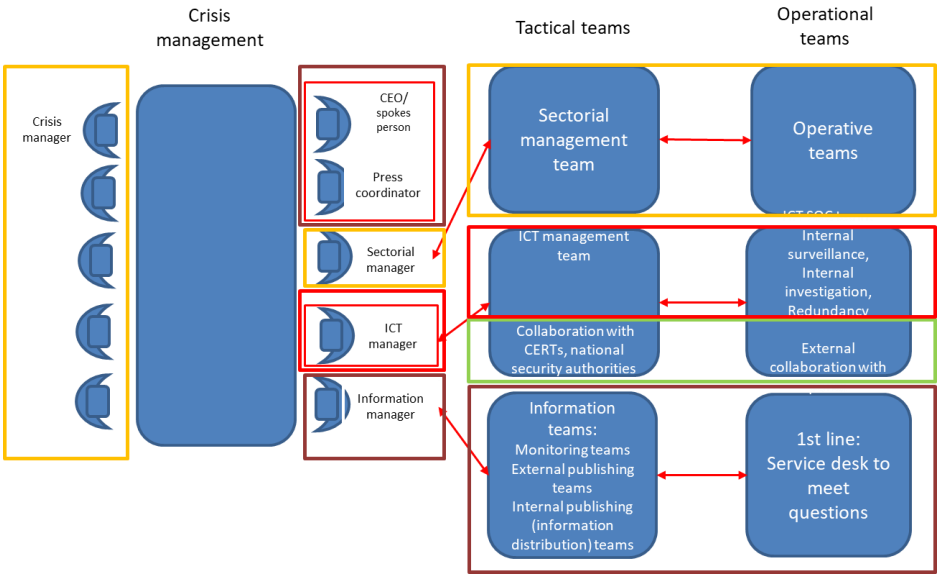



**Fig. 14.** Hvem skal trenes? [36]

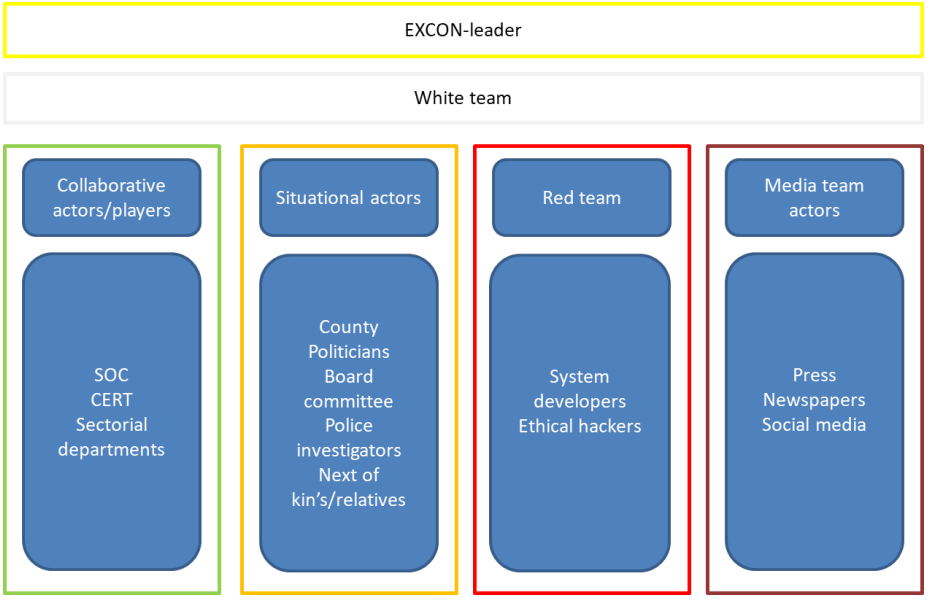



**Fig. 15.** Spillstab for øving av de som skal trenes [36]

Dette må selvfølgelig bygges opp basert på hva slags organisasjon som skal øves og hva slags øvelse som skal gjennomføres.

Slike øvelser kan koordineres (i henhold til mandater) av Statsforvalter og NSM i samarbeid med ulike cyber-range miljøer, eksempelvis Norwegian Cyber Range/NTNU på Gjøvik.

### Krysskoordinering

Krysskoordinering (regulert) fra lokal koordinering (Statsforvalter) og nasjonale myndigheter (Nasjonal sikkerhetsmyndighet) i slike angrep kan til tider skape forvirring og usikkerhet. Som vi ser av intervjuene var Statsforvalter inne i kriseledelsen, men hadde lite å gjøre med de taktiske og operative IKT-teamene. NSM og andre fra Felles cyberkoordineringssenter var i liten grad i dialog med kriseledelsen (noe var det, men ikke mye), men de var ved flere anledninger i kontakt med IKT-teamene både på taktisk og operativt nivå. At NSM sørget for at øvrige aktører ved Felles cyberkoordineringssenter kom i kontakt med «de rette menneskene» i Østre Toten for å få den informasjonen de trengte ble nok gjennomført etter beste evne, men det er mulig NSM burde hatt noe mer dialog med kriseledelsen, slik at kriseledelsen kunne fått muligheten til å delta i prioriteringen av informasjonskravene. I så måte kunne man også sett på muligheter for bedre dialog for prioritering mellom Statsforvalter og NSM. Er det konsekvensene for befolkningen eller informasjonskravene som skal prioriteres? Med andre ord de litt mer overordnede sosio-tekniske faktorene for organisasjonen, 1) Struktur, 2) Kultur, 3) Metoder og 4) Maskiner (se figur 9).

## Kort oppsummering og fremtidige vurderinger

Denne rapporten er laget for å gi organisasjonen i seg selv og andre organisasjoner læring. Samtidig vil erfaringene fra hendelsen kunne knyttes opp mot undervisning og øvelser. Rapporten beskriver situasjonen som den er, og hvordan man bør forberede seg dersom tilsvarende skulle skje i egen organisasjon.

Rapporten omfatter imidlertid ikke samfunnsperspektivet, deri den spente situasjonen mellom øst og vest, det at alle systemer er knyttet opp mot alt, teknologisk determinisme med dertil utmattelse i organisasjonene (da også ved sikkerhetshendelser som denne), og ei heller noen form for motstridende tenking når det gjelder å sette seg inn i hvordan en nasjon gjennom hackergrupper kan eksempelvis sette viktige funksjoner i samfunnet ut av spill. Denne gangen var det en kommune som ble angrepet, hva om det samme skulle skje mot flere samfunnskritiske funksjoner samtidig? Å dra nytte av erfaringene fra denne hendelsen og finne synergier inn i scenarioer på regionalt og nasjonalt nivå vil også være en del av det framtidige arbeidet med opplæring, trening og øvelser.

# Referanser


[1] nettvett.no, "Løsepengevirus," *nettvett.no*, 2021. [Online]. Available: https://nettvett.no/losepengevirus/.

[2] Justis og beredskapsdepartementet, *Instruks for statsforvalteren og Sysselmesteren på Svalbard sitt arbeid med samfunnssikkerhet, beredskap og krisehåndtering*. 2015.

[3] J. Gilbrandt and M. Rønning, "Omfattende IT-angrep mot Stortinget," *dagbladet.no*, 2020.

[4] Nortura, "– Konsekvensene ble mindre enn de kunne blitt," *Nortura Medlem*, 2022.

[5] N. Rydne, "Slik håndterte Nordic Choice dataangrepet: – Det har vært tøft," *E24*, 2022.

[6] A. Krantz, M. F. Børresen, T. I. Hagen, and A.-K. Mo, "Dataangrepet: Kan skade korona-beredskapen," *nrk.no*, 02-Sep-2020.

[7] Cisco, "Annual cyber security report," 2018.

[8] Næringslivets sikkerhetsråd, "Mørketallsundersøkelsen 2020," 2020.

[9] S. Kowalski, "IT Insecurity: A Multi-disiplinary Inquiry," Stockholm University, 1994.

[10] G. Østby and S. J. Kowalski, "A case study of a municipality phishing attack measures - towards a socio-technical incident management framework," *CEUR*, 2021.

[11] G. ; Østby, L. ; Berg, M. ; Kianpour, B. ; Katt, and S. Kowalski, "A Socio-Technical Framework to Improve cyber security training: A Work in Progress," 2019.

[12] K. Scarfone, T. Grance, and K. Masone, "Computer Security Incident Handling Guide," 2008.

[13] Nasjonal Sikkerhetsmyndighet, "Rammeverk for håndtering av IKT-sikkerhetshendelser," pp. 1–20, 2017.

[14] NSR, *Nødplakat for digitale angrep*. 2022, p. 2022.

[15] Justis- og beredskapsdepartementet, "Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (sivilbeskyttelsesloven)." Norwegian Government, 2010.

[16] Norwegian government, *FOR-2011-08-22-894*. Norwegian Government, 2011.

[17] DSB, *Municipality guidance, emergency duty*. 2017.

[18] E. Deverell, *Crisis-induced learning in public sector organizations*. 2010.

[19] A. L. Fimreite, P. Lango, P. Lægreid, and L. H. Rykkja, *Organisering, krisehåndtering og samfunnssikkerhet*. NO: Universitetsforlaget, 2014.

[20] J. Birkinshaw, "Making sense of knowledge management," *Ivey Bus. J.*, vol. 65, no. 4, 2001.

[21] B. Mishra and A. U. Bhaskar, "Knowledge management process in two learning organisations," *J. Knowl. Manag.*, vol. 15, no. 2, pp. 344–359, 2010.

[22] M. Easterby-Smith, M. Crossan, and D. Nicoliny, "ORGANIZATIONAL LEARNING: DEBATES PAST,PRESENT AND FUTURE," *J. Manag. Stud.*, vol. 37, no. 6, 2000.

[23] D. A. Schon, "Deutero learning in organizations: Learning for increased effectiveness," *Organ. Dyn.*, vol. 4, no. 1, pp. 2–16, 1975.

[24] R. A. Myer, C. Conte, and S. E. Peterson, "Human impact issues for crisis management in organizations," *Disaster Prev. Manag. An Int. J.*, vol. 16, no. 5, pp. 761–770, 2007.

[25] D. West-Brown, Moira J. Stikvoort, G. Killcrece, R. Reufle, and M. Zajicek, *Handbook for Computer Security Incident Response Teams (CSIRTs)*, 2nd ed. Carnegie Mellon Software Engineering Institute, 2003.

[26] G. Parmigiani and L. Inoue, *Decision Theory: Principles and Approaches*. UK: John Wiley & Sons, 2009.

[27] S. Kowalski, T. Grunnan, and M. Maal, *A socio-technical model of a post disaster and crisis management learning process.* 2014.

[28] G. Østby and S. J. Kowalski, "Preparing for Cyber Crisis Management Exercises," in *n: Schmorrow D., Fidopiastis C. (eds) Augmented Cognition. Human Cognition and Behavior.*

*HCII 2020. Lecture Notes in Computer Science, vol 12197.*, 2020, pp. 279–290.
[29] G. Wahlgren and S. Kowalski, "A Maturity Model for IT-Related Security Incident Management," in *Business information systems*, Springer, Cham, 2019.
[30] G. Wahlgren and S. Kowalski, "IT Security Risk Management Model for Cloud Computing," *Int. J. E-entrepreneursh. Innov.*, vol. 4, no. 4, pp. 1–19, May 2014.
[31] H. W. L. Sweet, R. K. Edwards, G. R. Lacroix, M. F. Owens, and H. P. Schulz, "A Method for Assessing the Software Engineering Capability of Contractors," 1987.
[32] W. Kuechler and V. Vaishnavi, "A Framework for Theory Development in Design Science Research: Multiple Perspectives," 2012.
[33] G. R. Karokola, "A framework for Securing a-Government Services, The case of Tanzania," Stockholm University, 2012.
[34] DSB, *Veileder til forskrift om kommunal beredskapsplikt*. DSB, 2018.
[35] G. Østby and B. Katt, "Cyber Crisis Management Roles – A Municipality Responsibility Case Study," in *Science and Technology in Disaster Risk Reduction in Asia*, 2019, pp. 168–181.
[36] G. Østby, K. N. Lovell, and B. Katt, "EXCON teams in cyber security training," *Proc. - 6th Annu. Conf. Comput. Sci. Comput. Intell. CSCI 2019*, pp. 14–19, 2019.
[37] KPMG, "IKT-sikkerhet i Østre Toten kommune forut for Sammendrag," 2021.
[38] G. Østby, S. J. Kowalski, and B. Katt, "Towards a Maturity Improvement Process – Systemically Closing the Socio-Technical Gap," in *6th International Workshop on Socio-Technical Perspective in IS Development - STPIS*, 2020, pp. 195–205.
[39] HSEEP, "Homeland Security Exercise and Evaluation Program Volume 1: HSEEP Overview and Exercise Program Management," 2006.
[40] DSB, *VEILEDER I PLANLEGGING, GJENNOMFØRING OG EVALUERING AV ØVELSER Metodehefte: Fullskalaøvelse*. 2016.
[41] ENISA, "Good Practice Guide on National Exercises," p. 80, 2009.
[42] M. E. Whitman and H. J. Mattord, *Management of Information Security*. Cengage, 2018.

# Vedlegg 1 - Mandat

I forbindelse med alle type hendelser som er av betydning, anmoder Statsforvalteren i det gitte området om å evaluere hendelser basert på sin instruks (forskrift) [2]. I Østre Toten sitt tilfelle ble det også tildelt skjønnsmidler fra Statsforvalteren, slik at ansatte skulle kunne frigjøres til å delta i evalueringen. Mandatet er her gjengitt i sin helhet:

*Nylige undersøkelser blant norske organisasjoner viser en økning i antall informasjons- og cybersikkerhetshendeleser, og ingenting tilsier at dette vil avta. Hendelser som cyber-angrepene mot Østre Toten kommune har satt en støkker i mange av oss, og mange sitter nå og lurer på hvordan sin egen organisasjon skal kunne håndtere denne type hendelser. Vi påstår at med hjelp av formidling av kunnskap i form av skolering, trening og øvelser, vil andre organisasjoner kunne dra nytte av det som har skjedd.*

*Ved NTNU sin Norwegian Cyber Range har de pågående et forskningsprosjekt omkring nettopp håndtering av slike hendelser. Kriselederansvaret i en kommune (og i andre offentlige organisasjoner) er jo fortsatt like klart som det alltid har vært gjennom lover og forskrifter, men de naturlige instansene for hjelp og støtte man finner i en «vanlig» hendelse er ikke nødvendigvis de samme som ved en informasjons- og cybersikkerhetshendelse. For eksempel kommer Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet (NSM) raskt på banen, da et cyber-angrep ikke nødvendigvis er lokalisert bare til kommunen det gjelder. I tillegg er det jo ikke bare system-sikkerhetshendelsen som skal håndteres, men også konsekvensene av angrepet - de øvrige hendelsene som oppstår. Eksempelvis i Østre Toten ble det som kjent i tillegg helt egne kriser i både skole, på aldershjem, i forhold til innkreving av avgifter, personopplysninger på avveie, mangel på tilgang til personinformasjon på NAV med mer.*

*Ved NTNU er det allerede publisert artikler om forskjellen i en slik hendelse sammenliknet med andre hendelser, og om hvilke ansvarlige aktører i samfunnet det er naturlig å knytte til hendelsen. Samtidig er det viktig å analysere hendelser som i Østre Toten for å se om prosjektets antakelser holder mål eller ikke, og for ikke minst å kunne gjøre endringer og forslag til en mest mulig optimal hendelseshåndtering i slike saker.*

*Målsettingen med evaluering av cyber-sikkerhetshendelsen i Østre Toten er å lære internt i kommunen av det som har oppstått, men også at andre skal kunne lære av hendelsen. Rammene for evalueringen av cybersikkerhetshendelsen skal utøves i en slik form at erfaringer og tilegnet kunnskap skal kunne benyttes i undervisning, trening og øvelser. Forskerne ved Norwegian Cyber Range forsøker nå å få oversikt over hva slags type aktuelle øvelser som eksisterer, og da spesielt innenfor lederansvar ved informasjons- og cybersikkerhetshendelser i offentlige beredskapsorganisasjoner. I et litteratursøk i forskningsdatabaser, alle høyt rangert innenfor informasjonssikkerhet, fant NTNU svært få resultater på øvelser innenfor ledelse av denne type hendelser. Kun 19 relevante akademiske artikler ble funnet, hvor ingen egentlig omfavnet alt i et slikt lederansvar som ligger i offentlige beredskapsorganisasjoner. Det var imidlertid viktige fragmenter i disse nevnte øvelsene som det blir viktig å ta med seg når øvelsene skal utvikles i tiden som kommer. Med andre ord er det skrevet*

*forskningsartikler basert på evalueringer om tilsvarende hendelser, men svært lite forskningsartikler er skrevet om hvordan man kan tilrettelegge for krisehåndtering fra et samfunnsmessig kriselederperspektiv, samt hvordan man best kan øve på slike hendelser for å være forberedt når de oppstår. Dermed ser kommunen det som viktig at ledelsen for evaluering av krisehåndteringen gis til NTNU Institutt for informasjonssikkerhet og kommunikasjonsteknologi ved forskere som spesialiserer seg innenfor dette feltet.*
*Evalueringen skal ta for seg hendelseshåndteringen av dataangrepet. KPMG har utarbeidet en rapport om datasikkerheten forut for hendelsen. Rapporten ligger på kommunens hjemmeside, her.*

*Kriseledelsen gir oppdrag til en evalueringsgruppe*

*Kommunens kontaktpunkt vil være kommunedirektør, men evalueringen vil i sin helhet bli ledet av NTNU.*

*Prosjektleder vil være Grethe Østby[2], PhD stipendiat ved NTNU Gjøvik, Institutt for Informasjonssikkerhet og kommunikasjonsteknologi. Grethe er under veiledning av Stewart James Kowalski [3], professor i Informasjonssikkerhet som jobber ved samme institutt.*

*Statsforvalteren i Innlandet og Statsforvalteren i Nordland vil delta som observatører. Ekstern kompetanse som har et bidrag ved denne type hendelser kan brukes, og de som hadde en rolle i hendelseshåndteringen vil delta i evalueringen (Statsforvalter, Kommune CSIRT, KS, politiet, NSM, PST, ekspertgrupper m.fl.):*
*Arbeidet skal:*

- *Få fram vesentlige læringspunkt fra hendelsen som kan gi grunnlag for å foreslå tiltak som kan styrke kommunens og andre kommuners kompetanse i håndtering av cybersikkerhetshendelser.*
- *Kartlegge håndtering av IKT-sikkerhetshendelsen hos Østre Toten kommune og vurdere hvordan håndteringen ble utført med utgangspunkt i lovverk og forskrifter:*
    - *Krav til risiko- og sårbarhetsanalyse i §3 i forskrift om krav til beredskapsplanlegging og beredskapsarbeid m.v. etter lov om helsemessig og sosial beredskap. Se også krav om forebyggende og skadebegrensende tiltak for å følge opp §4 og §9 i samme forskrift. De omhandler sikring av tilstrekkelig produksjon av tjenester ved mulige hendelser knyttet til avdekket risiko og sårbarhet.*
    - *Forskrift om kommunal beredskapsplikt: https://lovdata.no/dokument/SF/forskrift/2011-08-22-894*
    - *Personvern (GDPR)*
- *Kartlegge hendelsesforløp og involverte aktører*
- *Evalueringen skal omfatte krisehåndteringen, og foreslåtte sosio-tekniske metoder for rotårsaksanalyser av hendelseshåndtering ved informasjons- og cybersikkerhetshendelser skal ligge til grunn for evalueringen.*
- *I og med evalueringsarbeidet skal kunne brukes i forskning, så skal mandatet godkjennes ved Norsk senter for datasikring, og alle som tar del i undersøkelsen*

[2] https://www.ntnu.no/ansatte/grethe.ostby
[3] https://www.ntnu.no/ansatte/stewart.kowalski

*i form av spørreundersøkelser og intervjuer vil få et informasjonsskriv om forskningsaktiviteten i evalueringen, samt et samtykkeskjema de må signere på.*
- *KPMG har vurdert IKT sikkerheten i Østre Toten kommune forut for hendelsen. En skal vurdere om det er behov for ytterligere vurderinger av hvor godt forberedt kommunen var for å forhindre og oppdage angrep.*

*Evalueringsrapporten skal utformes slik at den blir ugradert, med eventuelle graderte vedlegg dersom dette er et behov.*

*Spørsmål som skal vurderes:*
1. *Hvilke aktører ble involvert i krisehåndteringen og hvordan ble den utført.*
2. *Bruk av beredskapsplaner, både generelle beredskapsplaner og spesielle innenfor informasjonssikkerhet (slik som kontinuitetsplaner), må vurderes opp mot faktisk hendelseshåndtering. Dette gjelder da også opp mot hjelpeaktører slik som Statsforvalteren, kommune CSIRT, NSM, PST etc.*

*«Hvilke mekanismer som utløses i forbindelse med håndtering av en hendelse kan derfor variere stort, og det kan være utfordrende for alle involverte å arbeide og samvirke optimalt når kompleksiteten og usikkerheten ved en hendelse er betydelig. Av den grunn er evaluering og læring etter større hendelser et nyttig virkemiddel for å bli bedre forberedt på framtidige hendelser (FFI-rapport s. 9 )»*

*Avgrensing*

*Evalueringsrapporten vil omhandle krisehåndteringen. D.v.s. ikke tekniske innstillinger på servere eller tekniske tiltak underveis. Imidlertid vil det være aktuelt å ta med hvilke beslutninger som ble tatt, hvem som tok disse, og ikke minst i samarbeid med hvem. Håndtering av IKT-sikkerhetshendelser omfatter forhold på ulike nivåer i organisasjonen. Det dreier seg om sikkerhetstekniske undersøkelser, metoder som benyttes i organisasjonen, struktur (kriseledelse, kommunikasjonslinjer etc.) og kultur i organisasjonen.*

*Metode*

*Metoden som vil benyttes er en kombinasjon av evaluering av hendelseshåndtering og sosio-teknisk analyse som beskrevet i fotnote[4]. I forkant av evalueringen vil Grethe gjennomføre en innføring i de to nevnte dokumentene som er vedlagt i dette mandatet. Informasjonsinnsamling: Dokumenter, logger, intervjuer og spørreskjema.*

*Framdrift*

*Evalueringen vil starte så snart mandatet er gitt, og søknad fra Norsk senter for forskningsdata (NSD) (for å få lov til å oppbevare data fra intervjuer etc. i perioden man analyserer disse). Normalt sett tar det ca. 3 uker for å få en godkjenning fra NSD.*

[4] G. Østby and S. J. Kowalski, "A case study of a municipality phishing attack measures - towards a socio-technical incident management framework," *CEUR,* 2021.

I løpet av perioden 13.01.2022 (dato for innsending av materiell til Norsk senter for datasikring (NSD)) – 01.05.2022 ble det gjennomført en større spørreundersøkelse samt 9 dybdeintervjuer for å dekke intensjonen i mandatet. I dialog med NSD hvor rammene for undersøkelsen ble godkjent, ble det i første omgang besluttet å avvente bruk av logger, da dette ville kreve helt andre rammebetingelser for gjennomføringen. Da hovedmålsettingen var at kommunen i seg selv, samt andre kommuner og organisasjoner skulle få læringsutbytte av hendelseshåndteringen med dertil forslag til tiltak for tilrettelegging for hendelseshåndering ved IKT-sikkerhetshendelser, har vi underveis sett at innhentet data i stor grad dekker intensjonen i mandatet.

# Vedlegg 2 - Resultater

Som en del av prosessen fikk vi en oversikt over totalt N=63 personer som hadde vært involvert i hendelseshåndteringen i større eller mindre grad. Av disse var N=31 ansatt i kommunen på tidspunktet hendelsen oppsto, mens øvrige var eksterne i form av myndigheter eller eksperter. Av de N=63 personene som sto på listen, aksepterte totalt n=38 å delta i forskningsprosjektet, hvor 25 av disse var ansatt i kommunen på tidspunktet hendelsen oppsto, mens øvrige altså var eksterne.

Av de n=38 som aksepterte å delta i forskningsprosjektet, svarte x=28 på hele spørreundersøkelsen og y=9 deltok i dybdeintervjuer. Av de x=28 som svarte på spørreundersøkelsen, så var 18 ansatt i kommunen på tidspunktet hendelsen skjedde, mens 10 var eksterne. Av de y=9 som deltok på dybdeintervjuer, var 7 internt ansatte, mens 2 var eksterne.

## Spørreundersøkelsen

Av de interne respondentene som svarte på spørreundersøkelsen, var det representanter fra politisk, strategisk (kriseledelse/toppledelse), taktisk (informasjonsteam/IT-ledelse/øvrig beredskapsledelse i org.) og operativt (IT-drift/IT-sikkerhet/øvrig drift i org. slik som leder ved sykehjem, leder ved skole etc.) nivå.

| Svar | Antall |
|---|---|
| Politisk | 1 |
| Strategisk (kriseledelse/toppledelse) | 4 |
| Taktisk (informasjonsteam/IT-ledelse/øvrig beredskapsledelse i org.) | 2 |
| Operativt (IT-drift/IT-sikkerhet/øvrig drift i org. slik som leder ved sykehjem, leder ved skole etc.) | 11 |

På spørsmål om hvordan cyber-angrepet påvirket den enkeltes hverdag, rent praktisk, svarte **politisk** respondent at «Epost og nett var borte. Kommuniserte bare med tlf de første dagen. I månedsvis var saksbehandlingskapasitet sterkt redusert», mens respondentene på **strategisk** svarte at «Alle systemer som jeg/vi bruker var nede. Måtte finne nye måter å løse utfordringen på, med å gjøre ting manuelt.», «Tok all fokus. Ansatte som måtte få tilpasset arbeidsforhold. Improvisere for å klare juridiske forpliktelser. Bruke privat epost og også sms i kommunikasjon med omverden. Mye kontakt med eksterne aktører, som var bekymret for at vi skulle sende virus over til deres systemer, og som ville stenge oss ute. Forsinkelser med rapportering og leveranser. Prosjekter som stoppet opp.», «All tid gikk til krisehåndtering både helhetlig i organisasjonen og i sektor, overordnet og operativt. Fokus på å holde driften gående og at innbyggerne i minst mulig grad skulle bli påvirket av angrepet. Mye uvisshet innledningsvis», og «Det er dette jeg har jobbet med det siste året. Veldig mange andre oppgaver har måtte vente.». På **taktisk** nivå svarte respondentene at «Alle fagprogrammer ble utilgjengelige og det førte til at alle arbeidsprosesser måtte foregå med manuelle rutiner. Det påvirket ikke tjenester til liv og helse», «For ordens skyld jobber jeg ikke i ØTK nå, men gjorde det på det aktuelle tidspunktet. Jeg jobbet som leder for digitalisering og innovasjon, en liten enhet med 3 hoder. denne aktiviteten stoppet naturlig nok opp, og jeg ble det vi kalte innsatsleder for arbeidet med

etterforskning, gjenoppretting og annet arbeid som skyldtes dataangrepet.», mens på **operativt** nivå svarte respondentene at «Alle dokumenter var lagret i fagsystem. Mistet tilgang til kritisk informasjon for å kunne utføre saksbehandling. Mistet muligheten til digital saksbehandling. Måtte lage nye rutiner for manuell saksbehandling.», «Ikke tilgang til arkiv, dette gjorde det umulig å behandle klager der en må ha tilgang til arkiv. Vedtak måtte skrives for hånd. Alt som skulle arkiveres, journalføres måtte skrives for hånd og oppbevares nedlåst til systemene var i gang igjen. Alt måtte da skannes inn. Elektronisk sikker kommunikasjon med leger, sykehus osv. måtte tas over telefon og skrives ned med papir og blyant. Dette medførte en betydelig økt tidsbruk. Likeledes ble vi kastet ut av Husbanksystemet, slik at Husbanksøknader ikke kunne behandles. Etterhvert fikk vi her etablert en løsning via NAV sine systemer. Brev måtte sendes ut manuelt.», «Manglende tilgang til oppgaver som skulle følges opp, endring i arbeidsoppgaver med fokus på krisehåndtering og bistå med å rigge sektoren for manuell drift samt driftsetting av systemene igjen i samarbeid med øvrige ansatte. Periodevis manglende tilgang til it systemene endret kommunikasjonsmåter hvor sms var eneste kommunikasjonsmåten med øvrige tjenester/funksjoner utenom fysiske møter.», «Min tjeneste fikk ikke utøvet tjenesten vi er satt til å gjøre. Det krevde mye koordinering i det å holde kontinuitet i tjenesten. Så ble det mye arbeid (koordinering) knyttet til gjennopprettingen.», «Jeg mistet tilgang til alle løsninger jeg brukte i hverdagen min, og derfor ble jeg hindret fra å gjøre jobben min. Ble etter hvert koblet til "dataangrepinnsats", og jobbet derifra med ikke noe annet enn gjenoppretting.», «Lange dager, kriseledelse og gjenopprettingsarbeid Alle dokumenter var borte. Måtte skrive alt på nytt. Måtte skrive referater osv med penn og papir. Ingen tilganger til systemer utover fagsystem som lå i skyen. Måtte kontere alle fakturaer for hele enheten med penn og papir. Ingen tilgang på printer/kopi/scanning. Ingen tilgang på mail første uken.», «Det snudde opp ned på hele arbeidshverdagen, vi måtte ta i bruk manuelle rutiner og det var en stor jobb å sikre at brukere fikk den hjelpen de skulle.», «tilbake til blyant og papir», og «mistet all tilgang til ressurstyringsverktøyet GAT. Var med på på å lage skjemaer for vaktbok, medisinark, legevisittark osv på papir Jeg startet noen få dager etter angrepet så hverdagen før er ukjent. Jeg fikk umiddelbart PC og tilgang til officepakken og e-post, men det var også det.»

Av de eksterne som deltok på undersøkelsen, jobbet 1 ved kommuneCSIRT, 3 i ekspertorganisasjon IKT-sikkerhet og 6 i andre type organisasjoner (man kunne også velge Statsforvalter, Datatilsynet, NSM, PST, men ingen fra disse organisasjonene svarte på undersøkelsen).

På spørsmål om hva bidro du med overfor Østre Toten kommune, rent praktisk, svarte kommuneCSIRT «Koordinering, rådgiving», mens ekspertorganisasjonene responderte med «Jeg jobber som innleid sikkerhetsressurs for KS, særlig som sikkerhetsansvarlig i Fiks-plattformen (bl.a. SvarUt). Jeg var kontakt med Østre Toten for å avklare om det var nødvendig å stenge kommunens tilgang til fellestjenestene på Fiks-plattformen. Dette er et tiltak vi bruker for å sikre at ikke disse fellestjenestene skal kunne misbrukes som angrepsvektor overfor andre brukere av Fiks-plattformens tjenester.
Jeg bistod kommunen i første omgang med å håndtere de personvernrettslige sidene av angrepet via rådgivning og utforming av diverse tekster. Jeg bistod også med gjenoppretting av fagsystemene sett fra et personvernperspektiv.», og «Var i lead fra Atea IRT fra angrepet ble oppdaget og de første dagene etterpå».
Fra «andre» type organisasjoner, ble det respondert med at «Jeg er ansatt som HR rådgiver i Gjøvik kommune, med ansvar for blant annet overordnet internkontroll og delansvar for styringssystem for informasjonssikkerhet. Østre Toten kommune rettet en

henvendelse til Gjøvik for å få bistand i rollen som personvernombud. Jeg ble "utlånt" i en periode som varte ca. 14 dager for primært å bistå med avviksmeldingen til Datatilsynet. Østre Toten opprettet personvernombud som tok over ansvaret på slutten av perioden jeg var utlånt. Det var en litt trå oppstart for PVO rollen: ikke opprettet kontaktperson for meg, dette kom på plass etter hvert. Det var lite fokus på praktiske rutiner og sikkerhet når fagsystemene lå ned: mottak, oppbevaring og avhending av personsensitive opplysninger. Jeg bisto i et oppstartsmøte med ansvarlige personer fra enhetene, hjalp til med pre-definering av ROS analyse som skulle gjennomføres i drift samt vurdering av personvernkonsekvenser. Det var utarbeidet en behandlingsprotokoll, som ikke var tilgjengelig i fasen jeg bisto. Alle enheter måtte derfor svare opp manuelt hvilke personopplysninger og personsensitive opplysninger som var behandlet i fagsystemene som ligger under deres ansvarsområde. Jeg måtte be om å få delta på møte med kriseledelsen for å bli koblet på håndtering av hendelsen. Jeg samarbeidet tettest sammen med Atea og Datatilsynet i forhold til rollen som personvernombud. Avviket ble avdekket 09.01.21, vi hadde tilstrekkelig informasjon til å sende inn avviket til Datatilsynet 13.01.21 (i den fasen vi var i da). Hadde kontakt med Datatilsynet pr. telefon i hele perioden jeg bisto kommunen.», «kommunikasjonsrådgivning», «Jobber ved IKT i Gjøvik kommune. Kommunene i regionen har felles nettverk så jeg var den som kuttet forbindelsen til ØTK den 9. januar, var det vel. I startfasen av hendelsen jobbet vi selv med å få kontroll og oversikt og utover i gjennopprettingsarbeidet koordinerte jeg mye av arbeidet mellom ØTK og Gjøvik av hvilke tjenester de trengte midlertidig tilgang til.», «Salg og prosjektering», «Gjennomgang av mulig infisert data.», og «Bisto innsatsleder med koordinering og håndtering av hendelsen, innleid fra KPMG.».

*Lærebokvurderinger av hendelseshåndteringen*
Innledende spørsmål baserte seg på hvilke strategier, policyer, daglig vedlikehold, risiko-analyser med dertil håndtering, samt utarbeidelse av beredskapsplaner innenfor informasjonssikkerhetsarbeid, en organisasjon kan utarbeide innenfor informasjonssikkerhet slik som Whitman og Mattord beskriver i sin lærebok innenfor ledelse av informasjonssikkerhet [42].

10 av respondentene hadde tidligere vært med på å utarbeide informasjonssikkerhetsstrategier for en kommune, mens 18 ikke hadde vært borte i slikt arbeid. 6 av respondentene kjente til at Østre Toten hadde informasjonssikkerhetsstrategi når cyber-angrepet oppsto, mens 22 av respondentene var ukjent med dette. Strategi var beskrevet som at det «gjerne er et skriftlig dokument som angir den langsiktige planen for innføring og oppgradering av informasjonssikkerhet i en organisasjon» 11 kjente til at Østre Toten kommune hadde informasjonssikkerhetspolicyer når hendelsen oppsto, mens 17 var ukjent med om dette eksisterte. Policyer var beskrevet at «består av skrevne instrukser på hvordan man gjennomfører spesifikke oppgaver innenfor en organisasjon. Og, at det kan bestå av overordnede føringer fra ledelse, standarder organisasjonen må forholde seg til, veiledninger og prosedyrer.»

De 11 som hadde svart at de kjente til at Østre Toten hadde policyer for informasjonssikkerhet fikk oppfølgingsspørsmål om hvilke typer policyer for informasjonssikkerhet de kjente til at Østre Toten hadde på tidspunktet hendelsen skjedde. Resultatene er presentert i tabell 2 (flere svar mulig).

Tabell 2

| Svaralternativ | Antall svar |
|---|---|
| Overordnede føringer fra ledelse | 3 |
| Krav til bruk av standarder innenfor informasjonssikkerhet | 3 |
| Veiledere innenfor informasjonssikkerhet (eksempelvis håndtering av GDPR, sikkerhetsklareringer etc.) | 8 |
| Prosedyrer for informasjonssikkerhet (med eventuelle retningslinjer for avvikshåndtering) | 5 |

På spørsmål om de kjente til om Østre Toten hadde et utarbeidet sikkerhetsprogram på tidspunktet data-angrepet skjedde, svarte 3 at de kjente til dette, mens 25 svarte negativt. Et sikkerhetsprogram var beskrevet som at «det består av en organisasjonsplan med dertil oppgaver/funksjoner som det er behov for, sertifiseringsprogram, utdanning, trening, øvelser m.m.» De 3 som svarte ja på undersøkelsen fikk oppfølgingsspørsmål om hva slags innhold de kjente til fra Østre Toten sitt sikkerhetsprogram. Disse resultatene er presentert i tabell 3 (flere svar mulig).

Tabell 3

| Svaralternativ | Antall svar |
|---|---|
| Funksjoner og arbeidsoppgaver var definert | 1 |
| Stillinger for å dekke funksjoner og arbeidsoppgaver var definert | 0 |
| Sertifiseringsprogram var definert | 0 |
| Krav til utdanning | 0 |
| Fast trening i organisasjonen | 0 |
| Øvelser | 1 |

På spørsmål om de hadde deltatt i risikovurdering av cyber-angrep mot kommuner, svarte 8 ja, mens 20 svarte negativt. 4 kjente til at det var gjort en risikovurdering av cyber-angrep før hendelsen, mens 24 svarte nei på dette. Av de 4 som kjente til at det var gjort en risikovurdering av cyber-angrep, svarte allikevel 1 at dette var utført på strategisk nivå, 1 at det var utført på taktisk nivå, mens 3 svarte at det var utført på operativt nivå. Det var derfor viktig å få kartlagt hva som faktisk var gjort i løpet av dybdeintervjuene.

På videre spørsmål om de var kjent med om det var gjort tiltak for å håndtere risikoen for cyber-angrep i Østre Toten kommune, svarte 5 at det var det gjort, mens 23 svarte nei. Tiltakene var beskrevet å kunne «være både organisasjonsmessige, kulturelle, nye metoder for informasjonssikkerhet eller sikkerhetssystemer på applikasjoner, systemer og maskiner.» Blant de 5 som svarte ja, mente 2 at det var gjort tiltak på taktisk nivå, og 3 at det var gjort tiltak på operativt nivå.

De samme 5 ble også spurt om hvilke tiltak som var gjort for å forbedre informasjonssikkerhetsrisikoen i Østre Toten kommune, og resultatene er presentert i tabell 4 (flere svaralternativer mulig).

Tabell 4

| Svaralternativ | Antall svar |
|---|---|
| Organisasjonsmessige tiltak (alt fra tilsetting av rett personell til å utføre rette funksjoner/oppgaver til å outsource systemsikkerhet) | 0 |
| Forbedre kultur for informasjonssikkerhet (løpende informasjon, trening, krav (sertifiseringer/klassifisering), øvelser) | 0 |
| Forbedre metoder for informasjonssikkerhet (eksempelvis prosedyrer med årlige oppdateringer, avvikshåndtering etc.) | 1 |
| Forbedre systemsikkerhet (apper, software, hardware ...) | 3 |

På spørsmål om de kjente til om Østre Toten kommune hadde en vedlikeholdsplan for systemsikkerhet når dataangrepet oppsto, svarte 6 ja, mens 22 svarte nei. En vedlikeholdsplan for systemsikkerhet ble forklart «å bestå av ekstern overvåkning, intern overvåkning (hva slags hendelser kan oppstå internt), plan- og risikovurdering, sårbarhets analyser og utbedring, beredskap og jevnlig gjennomgang av sikkerheten.» Blant de 6 som svarte ja, mente 1 at denne var kjent på strategisk nivå, mens 5 mente at den var kjent på operativt nivå.

Disse som svarte ja ble også spurt om hva slags vedlikeholdsplaner for systemsikkerhet de kjente til når hendelsen oppsto, og disse resultatene er presentert i tabell 5 (flere svaralternativer mulig).

Tabell 5

| Svaralternativ | Antall svar |
|---|---|
| Ekstern overvåkning av trusler | 0 |
| Intern overvåkning av trusler | 4 |
| Plan- og risikovurdering av systemer (informasjonsverdier, GDPR etc.) | 6 |
| Sårbarhetsanalyser og vurderinger (oppfølging av CAPEC, CVE, CWE, CCE, IT assets etc.) | 2 |
| Beredskapsplaner (hvem gjør hva når hendelsen oppstår) og jevnlig gjennomgang av systemsikkerheten | 3 |

På spørsmål om de hadde deltatt i utarbeidelse av beredskapsplaner for å håndtere cyber-angrep for kommuner, svarte 4 ja og 24 nei, og på spørsmål om de kjente til om Østre Toten kommune hadde utarbeidet beredskapsplaner for cyber-angrep, svarte 1 ja og 27 nei. Den ene som svarte ja på at det var utarbeidet beredskapsplaner svarte også på hvilke beredskapsplaner for å håndtere cyber-angrep i Østre Toten kommune vedkommende kjente til. Dette er presentert i tabell 5 (flere svaralternativer mulig).

Tabell 5

| Svaralternativ | Antall svar |
|---|---|
| Plan for hendelseshåndtering på operativt nivå (systemteknisk) | 0 |
| Plan for hendelseshåndtering på krisehåndterings nivå (som i hendelsen) | 1 |
| Eskaleringsplaner (fra operativt, til taktisk, til strategisk nivå) | 0 |
| Eskaleringsplaner (anmelde til politiet, melde til Statsforvalter, Datatilsynet etc.) | 0 |
| Planer for å innhente eksperthjelp | 0 |
| Kontinuitetsplaner (plan for bruk av redundante systemer, back-up, manuelle verktøy) | 0 |
| Informasjonsplaner (internt og til media) | 1 |

*Lovpålagte krav til samfunnssikkerhet og beredskap i kommunene*
De neste spørsmålene omhandlet lovpålagte krav til samfunnssikkerhet og beredskap i kommunene (Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret [15], forskrift til loven [16] og veileder til forskriften [34]).

På spørsmål om Østre Toten kommune har kartlagt hvilke uønskede hendelser som kan inntreffe i kommunen, vurdere sannsynligheten for at disse hendelsene inntreffer og hvordan de i så fall kan påvirke kommunen basert på risiko- og sårbarhetsanalyse ihht. Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (Sivilbeskyttelsesloven) §14, svarte 12 ja, 2 nei, og 14 vet ikke.

På oppfølgingsspørsmål til de 12 som svarte ja om risiko- og sårbarhetsvurderingen ble gjennomgått ved siste revisjon av kommunedelplaner i henhold til Sivilbeskyttelsesloven §14, svarte 4 ja, 0 nei og 8 vet ikke.

På spørsmål om cyber-angrep som hendelse var blitt vurdert i henhold til §14, svarte 1 ja, 4 nei og 7 vet ikke, og på spørsmål om cyber-angrep ble vurdert ved siste revisjon av kommunedelplaner svaret 1 ja, 3 nei, og 14 vet ikke.

På spørsmål om Østre Toten kommune beredskapsplan i henhold til Sivilbeskyttelsesloven §15, hvor beredskapsplanen skal inneholde en oversikt over hvilke tiltak kommunen har forberedt for å håndtere uønskede hendelser, hvor den som et minimum skal inneholde en plan for kommunens kriseledelse, varslingslister, ressursoversikt, evakueringsplan og plan for informasjon til befolkningen og media, svarte 10 ja, 0 nei og 8 vet ikke.

På oppfølgingsspørsmål blant de som svarte ja, om det var utarbeidet egne roller med definerte oppgaver i kriseledelsen for å håndtere et cyber-angrep, det vil si – om det var definert egne roller i kriseledelsen spesifikt for et cyber-angrep, svarte 2 ja, 4 nei og 0 vet ikke (6 svarte på oppfølgingsspørsmålene). Ytterligere 4 oppfølgingsspørsmål i henhold til veileder for hva en beredskapsplan ble stilt, og svarfordelingen er presentert i tabell 6

Tabell 6

| Spørsmål | Ja | Nei | Vet ikke |
|---|---|---|---|
| Er det utarbeidet manuelle varslingslister for bruk ved cyberangrep?<br>Eksempelvis at Statsforvalter, Datatilsynet og Politiet blir varslet. | 1 | 3 | 2 |
| Er det utarbeidet ressursoversikt til bruk ved cyber-angrep? | 1 | 3 | 2 |
| Er det utarbeidet en informasjons- og mediahåndteringsplan som kan brukes ved cyber-angrep? | 1 | 3 | 2 |
| Er det planlagt med hvem som skal uttale seg til media ved et cyber-angrep?<br>Det vil si - vil det bli brukt eksperter (internt eller eksternt) i tillegg til ordfører, som kan uttale seg om type angrep og situasjonsoppdatering omkring dette? | 1 | 0 | 0 |

På spørsmål om det det var utarbeidet egne roller med definerte oppgaver på taktisk nivå for å håndtere et cyber-angrep, eksempelvis kontakt med andre kommuner og helseinstitusjoner (gjelder teknisk etat, skoleetat, helse og omsorg og andre), kommuneCERT, politi (og deri evt. PST og NSM) (gjelder IT-ledelse), så var det ingen

som svarte på dette spørsmålet, dermed ble også åpent oppfølgingsspørsmål om hvilke roller og definerte oppgaver på taktisk nivå man kunne kjenne til heller ikke besvart.

På spørsmål om det var utarbeidet egne roller med definerte oppgaver på operativt nivå for å håndtere et cyber-angrep, eksempelvis kontakt med andre tekniske etater, skoler, sykehjem etc. (gjelder samarbeid operativt på tvers av kommunegrenser), eller eksterne SOC, CSIRT's, private ekspertoganisasjoner som Atea etc. (gjelder drift IT), svarte 1 ja, 1 nei og 2 vet ikke. På åpent oppfølgingsspørsmål om hvilke roller og definerte oppgaver for å håndtere cyber-angrep på operativt nivå de kjente til, ble det uttalt «Ingen kjennskap», «det er ikke definerte oppgaver spesielt for cyber-angrep, med for generelle kriseoppgaver», «skal møte opp på angitt sted ved bortfalle av kritisk infrastruktur. Gå over til manuell drift.», «jeg tenker at de som nå skal jobbe i vår IT avdeling (IDI), vil måtte håndtere et cyber-angrep.», «det er ikke utarbeidet eget planverk, varslingslister, tiltakskort eller lignende tilpasset cyberangrep, der har en "all hazards approach" tilnærming» «BCPT, CP, CPMT, CMPT, DRPT, IRPT Alle disse rollene/teamene har ulike oppgaver i en planlegging for kontinuitet i drift.», «Som jeg kjenner til, inneholder ikke kommunens beredskapsplaner noe som har å gjøre med cyberberedskap. Det finnes derfor ikke noen roller og oppgaver som spesifikt angår cyberberedskap.», «IKT avdeling og IKT leder», «vår beredskapsplan omtaler svikt/bortfall av elektronisk kommunikasjon. Kriseledelsen, fagpersonell, nøkkelpersonell, ekstra bemanning, kriseteam, beredskapsråd med frivillige.», «it – avdelingen» og «IKT avdelingen hadde avtale med ekstern leverandør som omhandlet håndtering av slike hendelser.»

*Sosio-teknisk tilnærming til hendelseshåndtering*
Spørsmål vedrørende hendelseshåndteringen ut ifra et sosio-teknisk tankesett ble presentert på oppstartsmøte og i mail til alle. Det ble også presisert at noen av spørsmålene som allerede er stilt også kommer inn under et slikt tankesett, slik at disse spørsmålene ville være utfyllende spørsmål vedrørende hendelseshånderingen - i en noe større sammenheng. For eksterne bidragsytere og samarbeidspartnere ble det formidlet at dette var de siste spørsmålene, mens det fortsatt ville være noen flere spørsmål til alle som jobber i Østre Toten kommune.

Roller respondentene hadde under krisehåndteringen av cyber-angrepet i Østre Toten kommune var fordelt på kriseledelse (7), taktisk ledelse (1), operativ ledelse (11), ekstern support uten operativmedvirkning (4), og ekstern support med operativ medvirkning (4)

I det følgende er de sosio-tekniske spørsmålene gjengitt i sin helhet, med definerte oppgaver innenfor hvert spørsmål.

I hvilken grad opplever du at det er god struktur for informasjonssikkerhet i Østre Toten kommune (tabell 7)?

Tabell 7

| (svar fordelt på antall) | Liten grad | Noen grad | Middels grad | Stor grad | I svært stor grad | Vet ikke |
|---|---|---|---|---|---|---|
| Klart definerte roller og oppgavefordeling i organisasjonen | 5 | 5 | 3 | 5 | 1 | 4 |
| Gode økonomiske rammer | 5 | 3 | 4 | 2 | 2 | 7 |
| Klar strategi | 6 | 4 | 4 | 3 | 2 | 4 |
| Gode policyer med dertil prosedyrer og system for avvikshåndtering | 3 | 6 | 5 | 3 | 2 | 4 |
| Den enkelte kjenner sitt ansvar innenfor informasjonssikkerhet | 4 | 9 | 2 | 1 | 0 | 7 |

I hvilken grad opplever du at det er god struktur for hendelseshåndtering ved cyber-angrep (tabell 8)?

Tabell 8

| (svar fordelt på antall) | Liten grad | Noen grad | Middels grad/vet ikke | Stor grad | Svært stor grad | Vet ikke |
|---|---|---|---|---|---|---|
| Klart definerte roller og oppgavefordeling | 4 | 3 | 3 | 8 | 0 | 5 |
| Bruk av krisehåndteringsplan | 5 | 2 | 5 | 2 | 1 | 8 |
| Bruk av kontinuitetsplan for informasjonssikkerhet | 5 | 3 | 2 | 3 | 1 | 9 |
| Bruk av ressurslister | 3 | 3 | 4 | 4 | 0 | 9 |
| Bruk av informasjonsplan for krisehåndtering | 1 | 2 | 6 | 3 | 1 | 9 |

I hvilken grad opplever du at det er god kultur for informasjonssikkerhet i Østre Toten kommune (tabell 9)?

Tabell 9

| (svar fordelt på antall) | Liten grad | Noen grad | Middels grad | Stor grad | Svært stor grad | Vet ikke |
|---|---|---|---|---|---|---|
| Det sendes ut jevnlig informasjon om typer av cyber-angrep som kan oppstå | 7 | 2 | 2 | 3 | 5 | 4 |
| Det gjennomføres jevnlig elektroniske kurs om informasjonssikkerhet (eksempelvis i forbindelse med sikkerhetsmåneded i oktober) | 5 | 6 | 6 | 1 | 0 | 5 |
| Det gjennomføres jevnlig seminarer om informasjonssikkerhet | 11 | 3 | 3 | 0 | 0 | 6 |
| Det gjennomføres øvelser innenfor informasjonssikkerhet | 10 | 5 | 2 | 0 | 0 | 6 |
| Det er tydelig hvor man skal melde fra dersom det er mistanke om brudd på informasjonssikkerhetspolicyer | 4 | 5 | 6 | 1 | 4 | 3 |
| Saker som blir meldt inn blir raskt tatt hånd om og tilbakemelding blir gitt til varsler | 5 | 4 | 2 | 2 | 2 | 8 |

I hvilken grad opplever du at det er god kultur for håndtering av cyber-angrep i Østre Toten kommune (tabell 10)?

Tabell 10

| (svar fordelt på antall) | Liten grad | Noen grad | Middels grad | Stor grad | Svært stor grad | Vet ikke |
|---|---|---|---|---|---|---|
| Åpenhet rundt hendelseshåndteringen | 0 | 2 | 1 | 9 | 11 | 0 |
| Informasjon til ansatte | 0 | 0 | 5 | 8 | 7 | 3 |
| Involvering av ansatte i håndteringen | 0 | 3 | 6 | 5 | 5 | 4 |
| Involvering av eksterne i håndteringen | 1 | 0 | 2 | 5 | 13 | 2 |
| Anmeldelse av hendelsen | 0 | 0 | 1 | 5 | 13 | 4 |

I hvilken grad opplever du at det er gode metoder for informasjonssikkerhet i Østre Toten kommune (tabell 11)?
(Totrinnsbekreftelse (autentisering) er et ekstra sikkerhetsnivå for innlogging. Med totrinnsbekreftelse logger du inn med noe du vet (ditt passord) i tillegg til noe du får (en kode på telefon))

Tabell 11

| (svar fordelt på antall) | Liten grad | Noen grad | Middels grad | Stor grad | Svært stor grad | Vet ikke |
|---|---|---|---|---|---|---|
| Regelmessig bytte av passord kreves | 2 | 0 | 1 | 11 | 3 | 6 |
| Det er ikke mulig å benytte gammelt passord ved opprettelse av nytt | 1 | 0 | 1 | 9 | 7 | 5 |
| PC-er har automatisk skjermlås etter kort tid | 1 | 4 | 0 | 4 | 8 | 6 |
| PC blir låst etter 3 feil forsøk med pålogging | 0 | 0 | 0 | 5 | 5 | 13 |
| Kommunen benytter to-trinns autentisering ved pålogging på online-systemer (som email, Transponder o.l.) | 5 | 1 | 3 | 0 | 9 | 5 |
| Hvis du benytter feil passord, blir du da rutet til to-trinns autentisering | 4 | 0 | 1 | 0 | 4 | 14 |
| Det er ikke mulig å logge seg inn på systemer med andres passord | 3 | 1 | 0 | 0 | 4 | 15 |

I hvilken grad opplever du at det er gode metoder for håndtering av cyber-angrep i Østre Toten kommune (tabel 12)?

Tabell 12

| (svar fordelt på antall) | Liten grad | Noen grad | Middels grad | Stor grad | Svært stor grad | Vet ikke |
|---|---|---|---|---|---|---|
| Systemer som er angrepet kan stenges av fra andre systemer | 4 | 0 | 2 | 2 | 1 | 14 |
| Back-up kunne benyttes etter kort tid | 8 | 5 | 0 | 1 | 1 | 8 |
| Logger kunne enkelt hentes ut for å gjenopprette data | 7 | 3 | 1 | 2 | 1 | 9 |
| Alternative systemer kunne benyttes | 8 | 2 | 1 | 2 | 1 | 9 |
| Alternative metoder (skriftlig, plakat på veggen, jevnlig info per telefon) kunne benyttes | 3 | 3 | 3 | 7 | 3 | 4 |
| Ble metoder for eskalering av informasjon om hendelsen benyttet | 3 | 0 | 1 | 4 | 3 | 12 |

I hvilken grad opplever du at det er god systemsikkerhet i Østre Toten kommune (tabell 13)?

Systemsikkerhet er sikkerhet opp mot både apper (online), software og hardware

Tabell 13

| | Liten grad | Noen grad | Middels grad | Stor grad | Svært stor grad | Vet ikke |
|---|---|---|---|---|---|---|
| Mailserver filtrerer bort (sandboxing) infiserte dokumenter | 2 | 2 | 2 | 5 | 2 | 15 |
| Apper (slik som Transponder) er innenfor brannmurer (DMZ) | 2 | 1 | 0 | 2 | 1 | 22 |
| Det er egne brannmurer på software (slik som øknomisystemer) | 3 | 0 | 0 | 2 | 1 | 22 |
| Det finnes en egen brannmur på min personlige PC | 2 | 0 | 0 | 4 | 3 | 19 |
| Det finnes egne brannmurer på web-sider (url-sikkerhet) | 3 | 1 | 0 | 1 | 0 | 23 |
| Ved systemoppdateringer så er det sikkerhetsvarsler, slik at du må oppdatere dine passord | 3 | 2 | 1 | 1 | 2 | 19 |

I hvilken grad opplever du den system-tekniske håndteringen av cyber-angrepet (tabell 14)?

| (svar fordelt på antall) | Liten grad | Noen grad | Middels grad | Stor grad | Svært stor grad | Vet ikke |
|---|---|---|---|---|---|---|
| Krypterte systemer ble sperret av fra andre systemer | 1 | 2 | 0 | 1 | 4 | 15 |
| Logger fra de avsperrede systemene ble etterforsket | 0 | 0 | 0 | 3 | 8 | 12 |
| Krypterte PC-er ble isolert og renset | 0 | 1 | 0 | 2 | 13 | 7 |
| Logger på/fra PC-er ble etterforsket | 0 | 1 | 0 | 3 | 2 | 17 |
| Ble kryptert hardware koblet fra strøm | 0 | 0 | 0 | 2 | 2 | 18 |
| Ble logger etterforsket på de isolerte maskinene | 1 | 0 | 1 | 2 | 2 | 17 |

*Modenhetsundersøkelse (eksalering og de-eskalering av informasjon under hendelseshåndtering)*

Spørsmålene i denne delen ble kun gitt til de som jobbet i Østre Toten kommune i forbindelse med hendelseshåndteringen, og omhandlet eskalering og de-eskalering av informasjon under hendelseshåndtering. Disse spørsmålene baserer seg på nylig utviklede modenhetsundersøkelser omkring nevnte [29], og går i noen grad mer i detalj enn tidligere spørsmål for å finne ut hvilket nivå organisasjonen er på. Resultatene fra denne undersøkelsen vil bli presentert i vitenskapelige artikler og Østby sin doktorgradsavhandling.

## Dybdeintervjuene

På politisk nivå i organisasjonen, ble det gjennomført intervju med ordfører, mens det på strategisk nivå ble gjennomført intervjuer med kommunedirektør og kommunalsjef for helse og omsorg. På taktisk nivå ble det gjennomført intervju med skolesjef og

økonomisjef, mens det på operativt nivå ble gjennomført intervju med personvernombud og utpekt innsatsleder IKT. Av eksterne ble fylkesberedskapssjef og en ekstern deltakende ekspert på hendelseshåndtering av cyber-hendelser intervjuet.

Ordfører i Østre Toten kommune, som har vært det siden 2019, var en del av kriseledelsen. Som ordfører og øverste politiske leder når data-innbruddet skjedde, så møtte han i kriseledelsen. Det var behov for mye intern og ekstern informasjon, særlig i forbindelse med den eksterne informasjon ut til presse og folket i Østre Toten, men og nasjonalt, som ordfører hadde en ganske stor rolle i. Ordfører fungerte som den folkevalgte representanten i kriseledelsen og hadde et overordnet ansvar for at beslutninger som ble tatt var innenfor «det som folk i Østre Toten kommune synes var greit». Det var viktig for ordfører som øverste politiske leder å fortelle om hendelseshåndteringen, og at det skjedde på en måte som ville være «ok» for folk i Østre Toten kommune, noe det ifølge ordfører var lite debatt rundt.

Kommunedirektør i Østre Toten kommune kom til Østre Toten 15. august 2020, altså et halvt år før cyberangrepet. I funksjonen kommunedirektør ledet han krisestab når den ble satt, da gjennom kriseledelsesmøtene. Første møte i kriseledelsen ble gjennomført lørdagsmorgenen, og det ble gjennomført møter jevnlig utover lørdagen og søndagen. I begynnelsen ble det gjennomført møter veldig ofte, og så ble det så ble det litt mer sjelden utover, men uansett en i gang i uka i over et år. Kommunalsjefene, økonomisjef, HR-sjef, beredskapskoordinatoren, ordfører, og representanter fra IKT var inne i så å si alle møtene. Men det var litt ulike roller de hadde etter hvert som hendelseshåndteringen utviklet seg. Sekretær var også til stede i disse møtene.

Kommunalsjef for helse, omsorg og velferd, var en del av kriseledelsen gjennom hendelseshåndteringen, og hadde det overordnede ledelsesansvaret innenfor sektorfeltet helse og omsorg. Som kommunalsjefen sa

> «I utgangspunktet skulle man jo tro at helse- og omsorgstjenestene er godt vant til å ha fokus på sikkerhet, da alle er vant til å forholde seg til taushetsplikten og har stor forpliktelse til oppfølging av de reguleringene. Og det er jo sånn at vi har bygd et nytt sykehjem for eksempel, som er teknologisk innretta. Vi har forhold i hjemmetjenesten som gjør at den daglige drifta er på digitale arbeidsplasser, og alt dette datt jo ned, så vi var på manuelle rutiner fra minuttet da dette skjedde. Vi var jo på manuelle arbeidsrutiner i lengre tid. Det gjorde jo at vi måtte tilbake til manuelle arbeidsrutiner som de hadde for veldig, veldig mange år siden. Penn og papir og kopimaskin, og telefax. På noen områder har vi hatt pasientsikkerhetsspørsmål, eksempelvis på Labo, som det er så mye teknologi med både pasientvarslingsanlegget, dykkesignalanlegget og dørautomatikk og den slags. Så blir det straks mer alvor ut av det da, og det gjorde det for så vidt i hjemmetjenesten og da, fordi der har vi jo elektroniske, det vil si digitale arbeidslister og når det ikke går an å få inn de lenger så da måtte vi dypdykke i søplekontaineren faktisk, slik at vi fant igjen noen lister som vi visste var kasta, og det er jo forskjell på intervaller på hvor ofte folk skal ha hjelp, hver 14 dag, en dag i uka, og da måtte vi da hente opp igjen de arbeidslistene. Det tok ikke veldig lang tid da, før det ble perm på perm på perm med papir, da alt vi vanligvis dokumenterer i elektronisk pasientjournal nå skal dokumenteres på papir i påvente at vi fikk opp igjen systemene. Jeg sa vel det til pressen en av de første dagene at

> dette er her surrealistisk, og det var det jo også. Jeg veit jo det at vi hadde prata om det helt løst i kommuneorganisasjonen at i framtida måtte vi forberede oss på at det ble flere hendelser, at ikke ustabiliteten ble så stor, og da ble det jo mer alvorlig da, så det så vi jo. Ja, og den dagen telefonen kom, så jobba vi jo hele den lørdagen, så da utpå ettermiddagen sa jeg at det eneste som mangler nå da er vel at strømmen går, og det gjorde den jo og. Det kom jo da melding utpå kvelden at strømmen hadde gått på Fjellvoll. Det var ganske spesielt, men jeg syns jo at det som har vært veldig imponerende er hvordan tjenesten har klart å holde hjula i gang, og vi har ikke fått noen meldinger om at det har vært noen alvorlige pasienthendelser, at det har gått ut over pasientsikkerheten, for ansatte har jobbet hardt for å holde oversikten selv om ikke alle opplysningene har vært tilgjengelig. Det er jo klart at vi har jo også hatt rutiner fra før på noe av det her, blant annet minimumskrav på at hovedkortet i journalen og medisinlistene, at det skal være utskrift av dem. Og det er jo nettopp med tanke på at det skal dette ned, så det har faktisk fungert bra.»

Skolesjefen er nærmeste leder for rektorene og de hadde jevnlig kontakt for å sammen finne løsninger på den enkelte skole i forbindelse med dataangrepet. Rektorene måtte håndtere de ulike utfordringene på sine skoler, med skolekontoret som kontaktpunkt. Skolen i Østre Toten bruker digitale løsninger på det meste av det de gjør, både når det gjelder skolekontoret med forskjellige programvare der og ikke minst ute på skole. Digitale ferdigheter er en av de fem grunnleggende ferdighetene som elevene utvikler gjennom hele skoleløpet. Disse er beskrevet i overordnet del i Kunnskapsløftet (LK-20). Disse ferdighetene er del av den faglige kompetansen og nødvendige redskaper for læring og faglig forståelse.

I tillegg til i undervisningen, benytter skolen i Østre Toten digitale løsninger til kartlegginger, dokumentskriving, skoleadministrativt verktøy, læringsplattform og arkivering. Og, som skolesjefen uttalte:

> «Grunnskolen hadde tatt i bruk Office 365 før 08.01.21, på tross av noe skepsis/ (motstand) fra kommunen for øvrig, da IKT-avdelingen mente at alle burde «gå i takt» her. Det at vi hadde vært såpass «fremme i skoa», ble noe av redningen for oss etter angrepet. Grunnen til at skole var mye lenger fremme enn resten av kommunen her, er at vi så nødvendigheten av å henge med i den digitale utviklingen for å gi best mulig opplæringstilbud til alle grunnskoleelever. En av de ansatte rådgiverne på skolekontoret, som er min stedfortreder, har blant annet arbeidsoppgaven med å være systemansvarlig for dataprogrammer, og han har mye med data å gjøre, så han ble jo veldig viktig i denne situasjonen her. Både for meg og for kommunen for øvrig, og også ute på skolen. Så han var jo en veldig god bidragsyter i denne prosessen her, og helt nødvendig.»

I Østre Toten er ifølge skolesjefen de dataene de har på elever lagret i deres skoleadministrative system som er en skyløsning. I tillegg har de manuelle elevmapper som oppbevares i låste arkivskap på skolene. Individuelle opplæringsplaner lagres i et system som også er en skyløsning, og dataene der var også sikkert lagret. Nevnte data var altså skånet for data-angrepet.

Mye av det den enkelte ansatte hadde lagret på sin egen maskin forsvant allikevel i angrepet. Selv om filene senere ble funnet og gjort tilgjengelig for alle ansatte en periode (slik at disse kunne hentes å lagres på et sikkert sted), var det likevel mange filer som ikke lot seg åpne/var forvunnet. Dette har medført en del merarbeid for lærere, skoleledere og også delvis skolekontoret (selv om de hadde det aller meste i onedrive), da mange dokumenter måtte memoreres så godt som mulig og produseres på nytt.

Økonomisjef er medlem av kommunedirektørens ledergruppe og var også en del av kriseledelsen under data-angrepet. Han ble tidlig kjent med hendelsen gjennom at it-sjefen var hans underordnet, og ble oppringt av ham da han var på vei til på jobb. Økonomisjef tok dermed ansvar for å samle kriseledelsen. Økonomisjef hadde også ansvaret for å melde hendelsen inn til Østre Toten sitt forsikringsselskap. Dette gjaldt blant annet KLP som var bekymret for at det de var utsatt for kunne spre seg igjennom dataflyt mellom Østre Toten og KLP. Gjøvik kommune som er vertskommune for det regionale ikt-arbeidet stengte Østre Toten ute fra gjensidig dataflyt umiddelbart. Husbanken samt flere andre statlige organer stengte Østre Toten ute av frykt for at det virus som kunne spres til deres organisasjoner, og som økonomisjefen uttalte:

> «Det var jo en viss form for kaos, hva var det vi var utsatt for og kunne det spre seg gjennom datatrafikk. Det var nok frykt hos mange.»

Personvernombudet startet i Østre Toten etter angrepet og fikk kort tid etter oppstart beskjed om at hun var ønsket som personvernombud. Før hun begynte i Østre Toten så var det en person som hadde rollen som hadde sluttet, og det var innleid bistand fra Gjøvik kommune frem til nytt personvernombud skulle på plass. Selv om personvernrollen er en liten del av hennes stilling, så ble det jo mye av den rett etter angrepet, og ikke minst når lekkasjen kom i påsken. Så når personopplysninger var delt på det mørke nettet så var hun veldig involvert. Avviket var allerede meldt Datatilsynet innenfor fristen, det ble gjort av økonomisjef, og da i samarbeid med personalsjefen som har ansvar for HR og kommunikasjon. Det som skulle meldes Datatilsynet, og i den grad man visste hva som egentlig hadde skjedd, deri hva som kunne være på avveie, ble håndtert et par dager etter angrepet. Dette ble gjort med bistand fra en person fra Gjøvik kommune. Når da nytt personvernombud startet, så ble det opprettet umiddelbar dialog med vedkommende fra Gjøvik om hvordan dette skulle følges opp.

> «Så satte jeg meg selvfølgelig til å lese igjennom forordningen, GDPR forordningen, og ut fra det spolet jeg meg inn på forskjellige personer i forskjellige nettverk, blant annet KS hvor jeg kunne få rask og effektiv hjelp, og ikke minst Datatilsynet. Jeg hadde veldig kjapt dialog med en fagleder på området i Datatilsynet, sånn at vi gjorde det vi måtte, men at vi ikke brukte mer tid enn vi var nødt for å håndtere det som skulle håndteres i forhold til Datatilsynet og eventuelle innbyggere. Og det var selvfølgelig også så viktig for meg i ombudsrollen å sørge for at vi fikk informasjon ut, altså at innbyggerne skulle bli satt i stand til å gjøre de tingene som er smarte for dem hvis det skulle ha konsekvenser, før vi visste at ting var ute.»

Personvernombudet var først med i kriseledelsen fra påsken når personsensitive data var delt på det mørke nettet. Det ble da opprettet kontakt med Datatilsynet, og det ble rigget for oppfølging umiddelbart. Personvernombudet var da i tett dialog med kommunedirektøren, med informasjonsrådgiverne på rådhuset, tett dialog med

Datatilsynet og med de som håndterte hendelsen (også KPMG). Det ble gjennomført daglige møter når de ble kjent med delingen på det mørke nettet. Det ble rigget en gruppe som skulle varsle innbyggere, under oppfølging av personvernombud.

> «Det viktigste for meg var jo egentlig den rollen min, å få opp en varslingsenhet, ja og jeg behøvde jo strengt tatt ikke å ha deltatt i den, men det er noe med hvem som deltar, hvem gjør dette fysisk, hvilken kompetanse er det lurt å ha på banen når vi skal begynne å varsle innbyggere. Det vi da var litt kjent med, hvor mye sensitiv informasjon, og om hvor mye det kunne være krevende for noen å håndtere, hva som var ute og gikk om dem da, for å si det på den måten. Så da var det da å bistå for å få rigget varslingsenheten, og så fortsatte jeg da å være delaktig i oppdateringsmøter gjennom hele påsken.»

Det var både jurister og ansvarlige fra KPMG som veiledet arbeidet, blant annet en person med solid kompetanse på sikkerhet og på sporing av hendelsesforløp. Kommunen fikk dermed hjelp til maskinelt å avlese det som ble kjent hadde lekket, hva som var lekket, men også hvem det er viktigst å varsle når, og hvor mye som bør varsles.

> «Skal vi varsle konservativt som er den ytterste konsekvensen ved å gå ut i media og si alt kan være ute og så stoppe det der, eller skal vi analysere litt her og lage en modell for hvem vi tar direkte kontakt med? Hvordan rigger vi det, her var det jo snakk om mange personer ikke norsk talende, hvor godt snakker de norsk, må vi rigge et tolke-apparat? Vi visste at det var lekket informasjon fra en 110-logg som egentlig ikke er informasjon unntatt offentlighet, men vi så jo der at det lå informasjon eksempelvis om at det var funnet døde mennesker på en grunneiers eiendom hvor brannvesenet rykker ut og de fører jo det i loggen. Det står jo ikke hvem, men det er klart at Østre Toten er lite så vi gjorde også noen vurderinger av det. Vi hadde med brannsjefen på den biten, og han sitter også i krisestaben. Vi vurderte det jo også sånn at vi i noen tilfeller varslet grunneiere også om at det har vært en hendelse og at det er ute på nett, selv om det kanskje ikke var sånn veldig sensitivt, så er det jo noe med ubehag og konsekvenser. Så vi var ganske romslige der. Vi måtte jo også sjekke, i og med at det var en del helseopplysninger, så måtte vi også bruke noe tid på å ha løsninger for å verifisere at vi snakket med riktig person. Det er sånn når du tror du ringer et damenavn og det er en mann som tar telefonen hver gang, forvisse oss om at vi snakker med riktig person, det var ikke like lett alltid.»

Kulturforskjeller, aldersbestemmelser og vergemål var også forhold som ble vurdert. En i varslingsenheten var i kontakt med NorSIS for å få deres anbefalinger på dette.

> «Men det var vi veldig tidlig, det var vel så fort verden hadde åpnet etter påske. Så hvis jeg kan si litt om det da, så synes jo vi vi gjorde en vanvittig jobb, så vi smilte jo litt i barten når det ukesvis etterpå så ut som om det var NorSIS som hadde kontaktet Østre Toten, og ja så det var litt interessant. Det var nok mange som ville pynte litt på brua si ja, når det gjaldt hvordan man hadde rigget seg. Men vi vi har jo dokumentasjon, jeg har logger fra hvert eneste møte, det skjønte jeg andre dagen i påsken at noen må lage et

konsept her for hvordan vi har håndtert dette her, så det tok jeg ansvar for det, så jeg har jo logger de første 3 - 4 ukene før hvert møte med hvem deltok.»

Varslingsgruppas hovedoppgave var å varsle de som skulle vite at ting som er konfidensielt for den enkelte er ute, og i ytterste konsekvens tapt for alltid. I varslingsgruppa var det en person fra voksenopplæringen, en person som tidligere hadde ledet krisestaben i Østre Toten med helsefaglig bakgrunn, og en kommunikasjonsrådgiver (i tillegg til personvernombud). Det ble utarbeidet en trafikklys-modell hvor de som var røde var de ble varslet en til en, totalt ca. 50 personer. Samtidig var det noen hvor det var en overvekt av gult som ble kontaktet, hvor summen av informasjon på avveie bestemte dette.

«Så var det å få tak i folk, da hadde vi (kommunen) helt tilfeldig bestilt utskrift fra folkeregisteret til et eller annet annet formål. Folkeregisteret er jo stengt i påsken og der er det ingen kriseberedskap. De kan også gjemme seg litt. Men tilfeldigvis var det en person som visste om denne utskriften, det tror jeg var kommunikasjonsrådgiveren som hadde oversikt over det, så den gruppa som ble satt sammen der det var det var kjempesmart.»

Etter at Norge åpnet igjen etter påske fikk de tak i noen ved Folkeregisteret, og fikk aksept for det for det de hadde av adresselister, for derved å kunne sende ut brev til alle innbyggere i Østre Toten kommune som var bosatt der på det tidspunktet. Både på norsk og engelsk, med henvisning til hjemmeside. I tillegg fikk alle de som ble ringt opp et eget brev.

«Vi kjente hverandre ikke, vi har aldri møtt hverandre, så vi begynte med en halvtime på teams hvor vi bare sånn kort dette er jeg flink til og dette er jeg flink til, og så var det en kjempematch. Og så diskuterte vi vanskelig saker. Og vi diskuterte også hvor mye vi kan gå ut med, der jeg for eksempel særlig knyttet til folk med psykisk altså psykisk utviklingshemming og sånn, hvor mye skal de selv vite, så vi hadde noen gode runder på det. Effektive gode runder. Og så loggførte vi selvfølgelig hvem har ringt hvor og når. Og når fikk vi taket i, fikk vi ikke tak i, svarte ikke på telefon, svarte på telefon. Vi kjøpte, det var det altså det er et verktøy som blant annet KPMG bruker til å bistå i sånne situasjoner, hvor du skal altså maskinelt avlese data, ja hvor de gjenkjenner etternavn, gjenkjenner personnummer. Det var et veldig godt verktøy, og der og da kunne vi jo bare bestille kolonner og sånt, for det vi trengte, så de modellerte det for oss.»

Innsatsleder IKT jobbet på daværende tidspunkt i Østre Toten kommune, hadde jobbet der i ca. 3 år, og var leder for det som ble kalt DIGIT, en relativt nyopprettet enhet, hvor det var 3 stykker som jobbet som prosjektledere innenfor de største digitale prosjektene innenfor innovasjon av teknologi/IT. Når hendelsen oppsto, så leste han som skulle bli utpekt som innsatsleder IKT, om hendelsen først i avisa før han fikk høre om det på andre måter. Det var så IT-sjefen som ville at han skulle bli med i et kort møte på søndag, sammen med en representant fra ATEA. Onsdag den påfølgende uken ble han utpekt som innsatsleder, mye på grunn av at det ikke var et prosjekt pågående akkurat da, og for å koordinere innsatsen i den fasen.

Statsforvalteren har ansvar for samordning når det skjer kriser, så det å følge opp kommunene både med øvelser og ved innsatser er vanlig oppfølging for dem. Når det gjelder kriser følger de opp behov for støtte og hjelp med nødvendige ressurser og eventuell samordning mellom kommuner. Fylkesberedskapssjefen, som representant fra Statsforvalteren, deltok i medlytt i møtene i kriseledelsen i Østre Toten kommune.

> «Da det jo er den rollen vi har, vi har jo også tiltakskort eller en strategi om du vil, på eventuelt når kommuner er i kriser, så tilbyr vi oss gjerne til å sitte på medlytt i kriseledelsen for å se om det er noe å bidra med da. Det gjorde vi jo gjennom pandemien når kommunene satte stab og hadde veldig store utbrudd, så hadde vi jo folk som deltok i kriseledelsene, og når Østre Toten ble rammet så var det jeg som satt som liason, eller som støtte, eller på medlytt i møtene i kriseledelsen i Østre Toten kommune.»

Samordningsansvaret handler om å sørge for at ressursene finner hverandre, og at alle som er involvert har den samme situasjonsforståelsen. Dersom det skal være tiltak på tvers av kommuner eller statlige etater så er det også Statsforvalteren som fasiliteter møtestrukturer for å få dette til. I noen hendelser er det veldig mange som skal inn og mene noe for å samordne tiltakene sine, mens i andre situasjoner er det mer isolert, og saken i Østre Toten var for Statsforvalteren mer av det isolerte slaget, da det kun råkte Østre Toten kommune.

> «I hvert fall sånn direkte, så er det jo sånn at for eksempel Østre Toten kommune samarbeider med andre kommuner, og man kunne derfor tro at eksempelvis Gjøvik eller Vestre Toten kunne bli rammet, så det er viktig å få de samtalene på plass og få kartlagt det og få greie på det. Men, det er jo mange andre bidragsytere også og det som ble gjort av samordning her, var nok for det første at vi tipset om kommune CSIRT, at de kanskje kunne være bidragsytere helt i starten, og de ble jo kontaktet, og etter hvert så var jo vår egen organisasjon, altså Statsforvalteren, spesielle spørsmål i denne saken her der vi har tilsynsmyndighet som måtte sørge for at kom inn i bildet blant annet forsvarlig helsetjenester og forsvarlig barnehagedrift da dataene deres var nede ganske lenge. Det var våre egne folk stort sett jeg var i kontakt med i denne hendelsen, det var ikke så mye ressurser som var påkrevd fra utsida som ikke kommunen selv har vanlig kontakt med da. Ja, jeg snakket med kommune CSIRT-en selv og. Ikke noe operativ utveksling, men at det nå skjedde noe som de måtte forholde seg til. Statsforvalteren skal sørge for at kommunene er i stand til å håndtere så mye som mulig selv, og dermed å snakke med dem og høre hva som står på, og om det er noe de trenger. Trenger de hjelp til noe, trenger de ressurser, har de ringt alle de folka man skal ringe når man gir tips om hvem det går an å prate med, og sørge for at de føler at de har noen i ryggen egentlig.»

Med bakgrunn i at Østre Toten en tid forut for hendelsen hadde gjennomført en modenhetsanalyse i samarbeid med ATEA (som en del av et helhetlig arbeid i Gjøvik-regionen), ble ATEA kontaktet når hendelsen oppsto (de hadde ikke en utarbeidet avtale med ATEA på dette, men en slik avtale ble da utarbeidet i løpet av en – to timer etter at de ble kontaktet). En sikkerhetskonsulent fra ATEA ble derfor raskt koblet på hendelsen. Vedkommende er til daglig medlem i ATEA incident responce team (IRT). Han hadde lead da ATEA IRT ble kalt inn på inn på hendelsen. Han satt i rollen som har kontroll på

alle aktivitetene som foregår ved «incident response» og da også informasjon oppover til ledelsen. Kontaktpersonen i kommunen på dette tidspunktet var IT-sjef.

> «Til å begynne med hadde jeg en sånn edderkopp funksjon siden vi jobber slik at vi undersøker saken først, og så finner vi ut hva slags type sak dette her, og så kaller vi inn våre ressurser etter hvilke ekspertområde de har, og så setter vi sammen et team, og til sist hadde jeg den overordnede oppgaven med å koordinere ting, så jeg bisto både med IRT og jeg bisto da også med informasjon og råd oppover.»

I tillegg til kontakt med IT-sjef, hadde ATEA også dialog med kommunaldirektør samt Visma og KS og også med NSM og Datatilsynet. Til å begynne med hadde de jevnlige møter for å finne omfanget av hendelsen, og de så fort at dette kom til å ta tid. De hadde lite å gjøre/lite å jobbe med fordi at det meste var tatt.

> «Det fantes noe brannvegg-logger, så det var vel møter 3 - 4 ganger i løpet av det første døgnet, og så var det det omtrent like mange ganger andre døgnet, men da var det jo også snakk om å briefe i forhold til presse og hva man skulle si og sånn.»

KS ville gjerne vite i detalj hva som hadde skjedd, deri hvor mye ATEA kunne klare å finne ut av angrepet, altså hvor lang tid det tok fra angrepet ble kjørt til systemene var låst. De var også interessert i sårbarheter i systemene, og de kom med noen anbefalinger et par uker i etterkant av angrepet. ATEA hadde imidlertid litt vanskeligheter med å forstå KS sin egentlige rolle, men fikk beskjed fra kommunen om å samarbeide med dem og å gi dem alt de ønsket. Det oppsto deri en usikkerhet omkring rollefordeling, og ATEA uttrykker en skepsis i forhold til om KS egentlig rådga kommunen godt.

> «Jeg tror det var mer til felles beste for alle kommuner, at de prøvde å finne noen felles trekk hvor man kunne gi et felles skriv.»

Underveis i prosessen så fant ATEA ut at på lagringssystemet, altså ikke på back-up-systemet men på lagringssystemet, så var det tatt et snapshot av alle serverne. Dette visste ikke kommunen selv noe om, men de fant dette såpass sent at de kun hadde 2 timer på å kopiere over det de klarte av viktige servere før det ble overskrevet. De hadde ikke mulighet til å stoppe overskrivingen fordi de har ikke nødvendige tilganger. Ergo ble de serverne de fikk beskjed om at det var mest kritiske kopiert, så langt det lot seg gjøre på de nevnte 2 timene. Og det var det de klarte å redde ut av data.

> «Ja bortsett fra «firewall». De hadde tatt back-up serveren. Det ATEA gjorde på den sårbarhetsanalysen, vi gjorde den siste analysen, var jo å påpeke da at de ikke hadde noe slags back-up av systemene, det var satt som veldig høyt kritisk at de ikke hadde det. Det ble laget et regneark med prioriteringer på hva kommunen måtte gjøre, men det rakk de da tydeligvis ikke å få på plass.»

Ifølge ATEA var det heller ikke gjennomført noen «business impact analysis» (BIA) på systemene (basert på at kommunen syntes å kun ha et visst begrep om hvilke systemer som var viktige), eksempelvis var det i kommunen en forståelse av at systemene ble benyttet ved sykehjemmene var viktige, men at systemer som ikke var vurdert var slikt

som låsesystemet og også systemlåser på medisinskapene. Dermed måtte de utstyre alle pasientene med bjeller, og med ekstra bemanning på gangen for å høre bjellene.

> «Det som gjorde at de fikk i gang noe, det var jo at de kunne på en få på plass PC-er og i alle fall bruke office 365 skyen som en som en plattform, men i begynnelsen så fikk de jo ikke kommunisert via email, så da var det private eposter det gikk på. Ja så det var jo det var jo helt nede. Det eneste om ikke var nede var «firewalen» og «switcher». Vi var jo ikke sikre på om de hadde vært inne på disse heller da, så vi anbefalte dem å kjøre clean install på alt sammen, i og med at vi ikke hadde noe logg på om det var kompromittert eller ikke. Angriperne hadde tydeligvis hatt tilgang på administratortilganger, og mot våre anbefalinger da så hadde de jo AD-integrert (Active Directory Integration) på det meste, at du dermed får tilgang til back-up via admin kontoer. Du får da tilgang til VMV-er via admin kontoer, og det er ikke det vi anbefaler alle fall.»

Det var en tidligere ansatt som var hyrt inn for å hjelpe til med brannveggen (hadde fortsatt tilgang selv om vedkommende ikke lenger var ansatt i kommunen). Dette gjorde at de kunne få litt logger fra brannveggen. Det var brukere og passord som hadde ligget der lenge, altså som aldri hadde blitt skiftet på enkelte enheter, dette være seg «appliances» som var «firewall appliances», «switchere», rutere og liknende, samt at det var en del fagsystemer som hadde lokale baser som det ikke var passord policy på.

> «Det var jo 2 hoder da for it avdelingen + IT-sjef, og det var det er jo begrenset hvor mange hatter de kan ha, og hvor mye de klarer å utføre på en måte. Og de hadde jo ikke overvåking av systemene på noen måte, i hvert fall ikke noe SIEMS verktøy eller noe.»

ATEA brifet allikevel ift. hva de så om de mulige angreps-vektorene de fant, også da med hensyn til påvirkning på tjenester hvor de kunne se om de kunne klare å få det opp igjen et nivå. Det ble formidlet at det kunne komme til å vare en stund, gjerne måneder, fordi de var helt på bar bakke. ATEA satte dog opp et system for å vaske data, det vil si at de tok de kompromitterte dataene som de fant fra «snapshoten» på lagringssystemet, for deretter å kopiere data over til en midlertidig løsning som vasket dataene og sjekker dem for ulumskheter, og deretter kopierte videre dataene til et nytt reinstallert system. Den prosedyren ble iverksatt mens sikkerhetskonsulenten fra ATEA var i lead.

ATEA satte altså i gang prosedyrer og fikk i gang et apparat i ATEA så de kunne avhjelpe kunde, hadde en prosjektleder på det, og stilte i utgangspunktet med nødvendige ressurser for å komme fortest mulig i gang igjen med de systemene som var viktigst. Eksempelvis vasking av data ble delt opp i områder hvor ekspert-konsulenter fra ATEA kunne hjelpe Østre Toten med å få på plass data. I tillegg for å få på plass nye maskiner hvis dere trengtes, da man på dette tidspunktet ikke visste om hele serveren kunne være kompromittert, og at det da går det raskere å få tak i nye servere for å gjenopprette arbeidet. Østre Toten hadde en del eldre servere som ikke var koblet mot nett, som man kunne bruke til å reinstallere programvare på. Fokuset var å få systemene opp i drift, med prioritet på de viktigste systemene (kritiske for liv og helse). Kriseledelsen gjorde en prioritering av hvilke systemer som skulle først opp. Dette baserte seg på liste/excel-ark med systemer i prioritert rekkefølge. Listen ble etter kort tid redigert noe for å få på plass eksempelvis nevnte låssystemer. Kriseledelsen var ifølge ATEA mest

opptatt av pasienter og liv og helse. Men også i tillegg, fordi ATEA avdekket i samtaler med VISMA at del-systemet på deres side på den tiden ikke var kryptert godt nok. Der var det kun brukernavn og passord som var kryptert, mens pasientdata/persondata ikke var kryptert i databasen, slik som kommunen trodde. På dette tidspunktet var team fra ATEA inne på det mørke nettet og så sa at det var det var publisert at noe hadde blitt tatt, men det var ikke lagt ut noe ennå. Dette ble kommunisert til kommunedirektør og IT-sjef. For øvrig hadde sikkerhetskonsulenten en eller to samtaler med Kripos hvor vi påpekte hvilken det mørke nettet det lå på. Det var kommunen som anmeldte forholdet og ATEA ga bare noen detaljer til Kripos. Også NSM var i kontakt med sikkerhetskonsulenten for noen detaljer.

*Hvem var dine ulike kontaktpersonene i Østre Toten kommune (hvem ble det eskalert eller de-eskalerte informasjon til)? og Var du kontaktperson for noen utenom Østre Toten kommune (eksempelvis for etterforskning eller annet)?*

*kommentar: Svar på første og andre spørsmål her overlappet i stor grad, derfor er svarene slått sammen under en felles bolk.

Ordfører var hovedsakelig i kontakt med IKOMM og kommunedirektøren og forskjellige typer media, samt med kommunestyret og formannskapet. I formannskapet var det orienteringspunkter fra ordfører og kommunedirektøren. Hendelseshåndteringen ble gjentatte ganger presentert i kommunestyret for å stadfeste og få aksept på at dette ble håndtert på en «akseptabel» måte, spesielt med bakgrunn i pengebruk. Det ble også tatt noen valg om hvordan IKT-drift og sikkerhet skal organiseres, særlig med tanke på å kjøpe drift av tjenester fra IKOMM, som også ble presentert i kommunestyret. Både kostnadene i seg selv, og også hvordan en endring av struktur for drift av systemene var beslutninger som kommunestyret må ta, i tillegg til å vurdere en del ekstra kostnader som du dukker opp underveis, med tanke på kompetansebehovet.

> «Hva du skal ha på hjemmebane utenom IKOMM for å ivareta sikkerheten våres fremover? Ikke bare sikkerheten, men digitaliseringskapasiteten kan du si da. At du har en slags oversikt over det og hva slags kompetanse på det som er slik at Østre Toten kommune gjør det på en fornuftig måte. Vi kan ikke bare gjøre det slik som andre kommuner gjør, vi må tenke på våre egne behov, og bestille fra IKOMM, og tenke på vår egen utvikling på det området her da. Det går både på digitaliseringskapasitet og sikkerhet, egen sikkerhet da. Så der har vi ansatt en del folk, så jeg tror vi bruker like mye penger på dataavdelingen vår nå, selv om vi har outsourcet. Så vi bruker like mye her hjemme nå som vi gjorde før datainnbruddet. Det er en helt annen situasjon og en helt annen kapasitet på den avdelingen nå da. En helt annen kunnskap. Min oppgave og kommunestyrets oppgave er at de beslutninger som innebærer bruk penger og som involverer på en måte å godkjenne den måten å gjøre det på som kommunedirektøren på en måte egentlig har bestemt, det er jo fagkunnskap ikke sant, og vi har veldig tillit til måten som kommunedirektøren har løst det på, og det gjør at det har vært lite debatt på en måte i kommunestyret fordi på en eller annen måte så har vi fått til det at kommunedirektøren har hatt god tillit og har hatt trua på at vi skal løse dette her.»

Ifølge ordfører var det stor enighet i kommunestyret om måten å gjennomføre arbeidet på.

> «Mye var rundt hvordan vi startet med kommunikasjon eksternt og internt den dagen vi ble rammet av det. Jeg tror at det er en sammenheng med at det er vært ganske troverdig og inngitt tillit tross alt. Derfor har vi fått ganske stor tillit i kommunestyret. For det er jo en ganske stor mulighet til å miste tillit da, når du ikke klarer å passe på dataene dine. At du ikke klarer å unngå at noen bryter seg inn hos deg, så er det en veldig stor mulighet til å miste tillit og det blir veldig, veldig stort behov for å gjenopprette den tilliten, og det er mye lettere å miste sitt gode rykte enn å gjenopprette det da. Men jeg tror det har klart å beholde tillit gjennom intern og ekstern informasjon, det har vært ganske stor ro rundt dette her, ganske tverrpolitisk enighet om gjenopptak, ja gjenopprettelsen.»

Ifølge kommunedirektøren var det ingen plan for å ha IKT-personell i kriseledelsen. IT-sjef ble allikevel innkalt i kriseledelsen når hendelsen skjedde, for å gi status på gjenopprettingsarbeidet. Etter hvert så ble det utpekt en ansvarlig for hendelseshåndteringen på IKT. Da ble møtte han i tillegg i kriseledelsen sammen med IT-sjef.

> «De ga status i forhold til; i begynnelsen så var det jo beskrive hva som hadde skjedd, og så etter hvert så var det jo status i forhold til gjenoppretting og når vi kunne forvente å få systemer oppe da. Og etter hvert som vi etablerte oss og fikk se omfanget så var det jo prioriteringer om hva som skal gjøres først.»

Kriseledelsen hadde da (under ledelse av kommunedirektør) Statsforvalteren i ulike møter, de hadde inne kommune-CSIRT som ga noen opplysninger sånn som de så det, og de hadde inne KS. Kommunedirektøren oppfattet at alle disse hadde en rådgiverfunksjon. Dernest ble det i noen grad delt i to, altså det som handler om IKT, gjenoppretning av systemene, hvordan for det første de skulle håndtere det. Og for det andre samtidig å jobbe med selve driften, hvordan driver man en kommune uten systemer, hvilke konsekvenser får det. Sistnevnte ble håndtert gjennom sektorene.

> «Nødprosedyrer og drift ble satt i gang, spesielt innenfor helse, omsorg og velferd. Det var jo veldig kritisk selvfølgelig. Men detaljene rundt det ble ikke tema i kriseledelsen. Det håndterte kommunalsjefen. Så var det spørsmål som gikk på tvers, for eksempel behov for vakthold, for beredskap og strøm, vi fikk jo også strømstans, så det ble behov for aggregater og sånn. Det var jo da tatt med eiendom og da hadde vi jo eiendom inne sånn som jeg husker det; når det var spørsmål om hvilken kapasitet vi hadde på aggregater, altså aktuelle problemstillinger da. Og så etter hvert som dette utviklet seg så var det jo organisert i forhold til dette med lekking av data, og da ble de jo tatt med inn i kriseledelsen når det var noen spørsmål angående det. Og så har det jo vært en veldig viktig ting og det går på informasjon. Vi har jo en informasjonsmedarbeider - en kommunikasjonsmedarbeider med hele veien selvfølgelig. I den første fasen så var det jo veldig mye informasjon både innad og utad som gikk på konkret på det og hvordan ansatte skulle forholde seg, og da var det vi hadde disse spørsmålene hva trenger vi, hvordan skal vi samle

> dette, og så ble den utførende biten gjort av de kommunale sektorene sammen med kommunikasjon.»

Kommunedirektør innrømmer at han ikke visste hvilke nasjonale ressurser som finnes innenfor informasjonssikkerhet, og at dette var noe han måtte finne ut av selv.

> «Så den jeg var i kontakt med, eller den jeg rådførte meg mye med var den som har et ansvar IKT sikkerhet i KS. Han kunne gi meg råd i forhold til da, hva trenger du av eksperter rundt deg, hvordan bør du organisere arbeidet, så det fikk vi veldig raskt på plass da.»

Spesielt gjaldt dette system-sikkerhet, hva man trenger rundt det, deri ekstern ekspertise. Dette arbeidet ble ikke ledet av kommunedirektør selv, men resultatet av arbeidet ble tatt med inn i kriseledelsen. Ett eksempel i denne forbindelse, var analysene av pågående og kommende gjenopprettingsarbeid, og deri anbefalinger fra eksterne eksperter på å følge et annet spor (outsoursing). Det rent tekniske var aldri kommunedirektør direkte borte i. Kommunen fikk også en ekstern henvendelse fra Cyber Forsvaret hvor disse bare ønsket å bli orientert, så ordfører og kommunedirektør hadde et møte med dem, hvor de informerte om det de visste. Det kom heller ikke noen gode råd eller tilbakemeldinger fra dem.

For øvrig var det kommunedirektør som anmeldte hendelsen til politiet i tråd av den delegerte myndigheten han har til å gjøre dette. Han hadde etter hvert som hendelsen skred frem mye kontakt med politiet. Det kommer her litt an på hvilken fase man er i, fordi da de leverte anmeldelsen, etter hvert som det kom spørsmål om dette med informasjon på avveie og misbruk av data, opplevde kommunedirektør at han hadde god dialog med politiet hele veien.

> «Vi fikk en del henvendelser fra publikum om «kan min bankkonto være misbrukt sånn og sånn» og hadde direkte kontakt med politiet og sendte de sakene over. Og vi fikk tilbakemeldinger om at de ikke hadde funnet noe som kunne knyttes til hendelsen da. Senere sent på høsten så ble jeg også invitert inn i et møte med NC3 altså Kripos NC3, hvor jeg fikk en orientering om etterforskningen rett og slett. Jeg tror kanskje at de som har ansvar for de tekniske undersøkelsene, vi hadde jo det som et eget spor, jeg tror kanskje de ga informasjon til Kripos, men det var ikke sånn som jeg var involvert i. Jeg ble kjent med at Kripos hadde skrevet en rapport om gjenopprettelsen og da vil jeg ha den rapporten, da vi mange runder for om vi skulle få den utlevert rett og slett. For å få vite hva de hva de visste.»

Skolesjef satt ikke i kriseledelsen, det var kommunalsjefen som satt der. Hun sitter i det de i Østre Toten kommune kaller BOO-ledergruppe (barn, oppvekst og opplæring). Denne gruppen hadde ledermøter med sin kommunalsjef, hvor det ble gjennomført beredskapsmøter og referert fra kriseledelsen. Skolesjef hadde jevnlige møter med rektorene der hun videreformidlet informasjon fra kriseledelsen fra kommunalsjef for oppvekst. Dialogen med andre slik som IKT avdelingen, gikk gjennom skolesjefens rådgiver, men det kunne til tider være krevende å «nå frem» med de spesifikke utfordringene som grunnskolen hadde. Det varierte ifølge skolesjefen litt, men det begynte med at skolekontoret hadde noe dialog med IKT avdelingen på rådhuset som hun hadde dialog med, men seinere i prosessen så hadde skolekontoret tett dialog med

gjenopprettingsansvarlig og IKOMM (i den grad de kunne gi de svarene skoleorganisasjonen trengte). Etter hvert ble det kun IKOMM som kontaktpunkt.

Han som ble utnevnt som innsatsleder IKT, koordinere all aktivitet som hadde med hendelseshåndtering IKT å gjøre, altså unntatt det som gikk innenfor den enkelte tjeneste i kommunen, hvor de måtte legge opp til manuelle rutiner. All koordinering rundt kommunikasjon, ekstern bistand, kommunikasjon med Kripos, NC3, NSM, etter hvert da med andre eksterne ressurser som de byttet ut med ATEA IRT (med ressurser fra KPMG) osv. Etter hvert kom det også på koordineringen med personvernsarbeidet, GDPR, rapportering på det, hvor innsatsleder IKT ble noe involvert i arbeidet med dette. I den gruppa var IT-sjef, den tekniske ressursen i kommunen som hadde mer eller mindre styring på gjenoppbyggingen av infrastruktur, og etter hvert kom en ekstern ressurs inn som arbeidet med juss-spørsmål, personvern og litt på GDPR, og også etter hvert eget personvernombud (innleid fra Gjøvik) som gjorde en del rapportering til Datatilsynet. Altså flere eksterne ressurser, men det var hovedsakelig KPMG sine hendelseshåndteringsfolk og etterforskningsfolk som satt i denne gruppen til å begynne med.

> «Vi hadde slike møter i begynnelsen hver morgen, etter hvert så gikk vi over til å ha det mandag, onsdag og fredag, og da skrev vi et levende referat fra hver gang på en måte i tilfeldigvis ei powerpoint-fil, og der er det en boks per område. Rådgiveren fra KPMG var på en måte min assistent, selv om jeg var kanskje like mye hennes assistent, for hun hadde jo erfaring fra faget og feltet. Vi to på en måte koordinerte dette sammen, og hun hadde da dialog med og hjalp meg med å kalle inn til møter og delta i møter med NC3 (Kripos) og NSM og også kommuneCSIRT til dels. Da var det jeg som deltok, det var henne og en rådgiver til fra KPMG som var en av de andre viktige i håndteringa som sto for den tekniske etterforskninga. Så vi fikk på en måte to hovedroller til, pluss at det var vi tre da som deltok i møter med NC3, NSM og ja, representant fra kommuneCSIRT var veldig pågående, så han fikk være med i noen av de møtene der. Han hadde jo ingen rolle i det, han var bare veldig klar og villig til å hjelpe, og veldig nysgjerrig på utviklinga, så han var med i noen av de samme type møtene da. Det som skjedde i de møtene, var jo bare at vi oppdaterte NSM og Kripos.»

Det var kontinuerlig overvåkning av darkweb fra eksterne ressurser (KPMG). Her også en som egentlig driver for seg selv med teknisk etterforskning, og ifølge innsatsleder IKT en av Norges beste eksperter på akkurat det, og i denne hendelseshåndteringen altså innleid fra KPMG. Han var ifølge innsatsleder IKT helt sentral i dette arbeidet, sammen med nevnte rådgiver («assistent») fra KPMG.

> «Litt sånn av historiske årsaker, og organiseringen og sånn, når vi ikke hadde møter i kriseledelsen, det hadde vi ofte for så vidt, da var det veldig naturlig for både meg og IT-sjef å snakke med økonomisjef, som satt i kommunedirektørens ledergruppe og som hadde lang fartstid og for så vidt beslutningsmyndighet ift. økonomi. Så vi drøftet jo veldig mye med ham i de tidlige fasene, for vi måtte jo, dette kostet jo en haug med penger som ikke var behandlet noen plass, så vi måtte bare ha en ryggdekning fra ham. Men ut over det, så var det i kriseledelsen som vi hadde møter i.»

På teknisk etterforskning så handlet det jo om å gi tilgang på data, det var behov for overføring av data (eksempelvis ifra et teknisk miljø til et annet), som ble koordinert og prioritert fra denne gruppen. Samtidig med etterforskningen bygde en i begynnelsen opp ny infrastruktur, så man var dobbelt avhengig av de samme ressursene. Dette innebar koordinering og prioriteringer og selvfølgelig kommunikasjon, hvor de hadde med seg kommunikasjonskonsulent fra kommunen. Vedkommende bidro til ekstern kommunikasjon, blant annet hjemmesider og media.

Sikkerhetskonsulenten fra ATEA hadde i tillegg til kontakt med IT-personell i kommunen, også kontakt med kommuneCSIRT. Dette ble beskrevet som mer en briefing av saken og hvordan og hva de hadde funnet ut underveis egentlig. Kommune-CSIRT-en var veldig interessert og ville gjerne få kjennskap til funn, og prøvde også å gi noe råd underveis, men det ble beskrevet at det var vanskelig å benytte seg av rådene siden alle systemene var nede.

Økonomisjef var i kontakt med Husbanken ved flere anledninger, men vi hadde også flere digitale møter med KLP som viste, ifølge økonomisjefen, en faglig forståelse, men også en kunnskap om hva kommunen var utsatt for. KLP stengte aldri ute kommunen fra sine systemer. Det gjorde imidlertid Husbanken og flere andre statlige organisasjoner. Spesielt i plan og bygningsmyndigheten som kommunen hadde forhold til, det vil blant annet si Kartverket.

> «Internt har jeg jo folka mine i avdelingen, vi måtte jo finne ut hvordan skulle vi kunne utføre det absolutt nødvendige av jobb når alt var borte. Så fant vi ut i fellesskap med Gjøvik kommune at vi kunne teknisk sett få tilgang til våre økonomi systemer og lønnssystemer som ikke var berørt av datainnbruddet fordi at systemene var driftet av Gjøvik kommune. Men vi hadde jo ikke tilgang til Gjøvik kommune, så den tilgangen var borte, men systemet var ikke berørt. Så da etablerte vi en midlertidig tilstedeværelse i Gjøvik rådhus for noen av folkene mine og noen andre folk, og så bygde IKT på Gjøvik en teknisk tilgang for noen av folkene våre slik at de kunne sitte i Gjøvik rådhus og jobbe på vårt økonomi-, personal og lønnssystem i denne her perioden. Og det klarte vi å etablere i løpet av en dag eller 2 eller 3. Det samme gjaldt også for ressursstyringssystemet for omsorgssvikt som ikke var berørt. Altså, de andre systemene som da ble driftet av andre enn Østre Toten kommune som i utgangspunktet var uberørt av datainnbruddet.»

Det var altså tilgangen til systemene som var borte, og det ble kommunisert med personell via telefoni eller privat mail i den første fasen. Økonomisjef sine primæroppgaver var tredelte, den ene var å sørge for at eget personell hadde muligheten for å jobbe. I utgangspunktet så kom de til et tomt Gjøvik rådhus på grunn av at det er var midt i corona-krisen, så det var jo hjemmekontor på stort sett alle ansatte i Gjøvik, mens de fikk lov til å disponere lokaler der. Dermed var det en del praktiske ting som måtte få på plass, så økonomisjef var mye innom på Gjøvik den første tiden. I tillegg var det personell med kompetanse på omsorgssystemet som også fikk jobbe fra Gjøvik. I tillegg deltok økonomisjef i kriseledelsen, og i ledergruppa som også var preget av denne situasjonen.

*Hva er det viktigste du lærte under hendelseshåndteringen?*

Ordfører:

> «Jeg har jo lært at IKT, jeg har jo kanskje lært det i fra før også, men man tar det for gitt da, at det ligger i bunnen for alle tjenester som kommunen har. Og kommunen har utrolig mange forskjellige virksomheter innenfor sin virksomhet da, selv om det er oppvekst og helse som er hovedoppgaven, så er det jo på plan og bygg og mange andre, altså det en mangslungen virksomhet. IKT er en sånn grunnkapasitet som vi visste vi var avhengig av, men var det litt overraskende at du er så avhengig av det allikevel. Og vi tar det for gitt da, så for 2 år siden kunne vi kanskje tenkt oss at vi skulle bruke mer ressurser på IKT og sikkerhet på IKT, men hvis vi skulle tatt det opp i kommunestyret ikke sant, så blir jo det satt opp mot lærere og sykepleiere og vanskelig å få flertall for å putte enda flere folk inn i rådhuset. For en kjenner seg igjen, når det skjer en sånn hendelse så har det vært mye lettere for oss putte ressurser inn i trygghet til en grunnleggende sikkerhet der, og jeg tror kanskje når vi har fortalt om dette til mange så er det gjort litt inntrykk sånn at noen andre kommuner og putter litt mer ressurser i sikkerhet. Nå var det jo noen manuelle rutiner som fungerte. Hvis du vet om en sykdom som en pasienter så er det jo kanskje en fordel å vite hva slags medisiner den har fått den siste måneden, og det hadde vi altså. De hadde rutiner rundt dette, så sikkerhet ble ivaretatt, men når IKT mangler, så er det jo så utrolig tungvint og det skal journalføres og alt det der, så det føles som å ikke ha det nesten da. Jeg tror at innbyggere i Østre Toten kommune nesten ikke har merket noen ting av det her. Fått regninger for sent og sånn, men dette har vært et problem for organisasjonen, for folk som jobber i Østre Toten kommune. Jeg tror innbyggere merket utrolig lite av det. Den vanlige innbygger som ikke jobber i kommunen. Noen har merket mer av det enn andre, men det har vært relativt lite merkbart og det kunne vært mye verre hvis datakapreren hadde offentliggjort mye mer. Da kunne det blitt en enda større utfordring, og det var en kjempeutfordring det i april, men kunne det vært mye verre. Mye mer ting som kan være mer sensitivt - at personopplysninger kommer ut om en av dem som er på læringssenteret og litte gran om det, og mange andre tjenester som har oppbevart mer sensitiv informasjon om folk. Byggstyring ble råket, og det var jo midt på vinteren og kaldt så det kunne jo vært fare for folk i disse byggene, og verdier i disse byggene hvis vi ikke hadde fått passet på. Så det kunne jo gått ordentlig galt med både folk og verdier.

Kommunedirektør:

> «Jeg vet ikke om du kommer tilbake til det, men når det gjelder lovverket rundt dette, altså kommunal beredskap, lov om kommunal beredskapsplikt sivile beskyttelsestiltak, og Sivilforsvaret, så er det jo sånn at jeg er kjenner jo til loven selvfølgelig, men disse lovkravene der, jeg har skjønt det sånn at det er et lovkrav på rapportering fra kommunens side ved hendelser, og detaljer rundt det har ikke jeg kjent til. Jeg har en beredskapskoordinator, og det er klart at når vi har en hendelse i kommunen så skal vi rapportere til Statsforvalteren og sånn, men detaljene rundt det, hvilke krav som lå til kommunen rundt det har jo blitt bedre kjent med i ettertid da.»

Kommunalsjef helse og omsorg:

> «Jeg sitter jo igjen med at det er ingen krise som er lik. For nå har vi jo hatt både den krisa og coronakrisa, og det er ingen krise som er lik, men det å se hvor ressurskrevende det her har vært det er i hvert fall en erfaring jeg tar med meg. Og så var jeg nok forberedt på at det kom til å ta tid å komme opp igjen og bli gjenoppretta, det så jeg også. Og så ser jeg jo at min egen adferd har endra seg når det kommer til detta her, jeg er jo ekstremt mye mere skeptisk, og mye mere reservert på å trykke på ting, og det gjelder jo både PC-er og telefoner og alt som er. Men så er det jo kanskje slik at du skulle ha trykt på den «greia der», og så blir det sånn så. Så både holdnings- og kompetansearbeid er det jeg har med meg i fortsettelsen, hvor viktig det er. Når det gjelder organisasjonen, så er det vel i enda større grad systemer som fanger opp denna risikoen og sikkerhet, men kanskje også mer automatisert systemovervåkning som går på sikkerhetsmonitorering og driftsmonitorering og ikke minst oversikt over hva vi har av utstyr rundt omkring og risikoen knyttet til det da. Det er jo et kjempestort udekket behov, og et kjempestort område å dekke. Og spesielt nå i et moderne digitalt samfunn, hvor folk jobber alle steder, vi har jo med pc-er, og mobiltelefon er jo med samme hvor vi er. Da handler det jo ikke bare om telefon eller pc-en, men det handler om hvordan håndterer du informasjonen som tilflyter om det så er på papir eller digitale flater da, hva gjør du med det? Det handler jo om grunnkompetanse, og så er det mye holdningsarbeid knyttet til det og.»

Økonomisjef:

> «Det er kanskje det kanskje 2 ting jeg har lært spesielt, og det ene er at det er deler av vår organisasjon som er har godt planverk for alternativ drift, spesielt i omsorg. Det er gjort planer for å kunne drive kommunen manuelt noen steder. Og andre steder var det å finne ut hvordan skal vi kunne drive en virksomhet som er digital, men som nå ikke er det. Hvordan skal vi da fylle våre forpliktelser overfor innbyggere, og også for leverandørene våre, og hvordan skal vi sikre økonomien til våre ansatte? Så vi la vel i utgangspunktet, i avdelingen min, så la vi jo i utgangspunktet alle sånne formelle ting veldig mye til side. Altså så improviserte vi, og jeg fikk jo nødvendige fullmakter. Kommunedirektøren ga meg alle fullmakter på vegne av alle ledere i Østre Toten kommune til å foreta fakturabehandling, for vi har jo en digital fakturabehandling. Det var kanskje 70 stykker som var involvert for at alle fakturaer skal bli kontrollert og attestert og anvist. Jeg fikk den ene fullmakten som jeg fikk lov til å delegere til regnskapssjefen slik at vi kunne utøve denne fullmakten i fellesskap. Så vi behandler jo alle fakturaer manuelt, men vi klarte å oppfylle forpliktelsen juridisk til å betale. Det var relativt mye arbeid. Vi hadde ingen mulighet for å kunne fakturere alle fakturaer ifra alle systemer, vi har jo vel av systemer som genererer grunnlag for det som til slutt blir en faktura. Selve fakturasystemet var operativt fordi at det var en del av dette økonomisystemet vårt som da ble driftet på Gjøvik, men grunnlaget som skulle komme i fra de øvrige systemet var dels borte. Så vi gikk et løp igjennom hele porteføljen for å finne ut hva det er vi klarer å få til og hva er vi da må informere om at vi ikke klarer å få til. Vi fant ut at ja vi kan få (fordi vi hadde

skyløsning på noen systemer som gjorde at etter at vi kom på bane IKT, altså vi fikk etablert epost system og sånn) så fant vi ut at vi kunne fakturere barnehageregninger og SFO-rgninger. Så det gikk ikke så veldig lang tid før vi kunne si at det her fakturerer vi normalt, mens dette her typiske - eiendomsavgiftene som vi kaller det, som da går på vann og avløp og sånn, også eiendomsskatt, det hadde vi ingen mulighet for å sende faktura på. Så da måtte vi forberede våre innbyggere på det, og noen var sikkert veldig glade, mens andre da ble på en måte bekymret for at de ikke fikk betalt regningene sine. Så vi hadde et opplegg for det, vi hadde énsides annonser i lokalaviser, og vi informerte veldig mye på hjemmesiden om det. Og i ettertid så viser det seg at innbyggerne våre var fantastiske til å takle at de i løpet av et halvt år, for vi begynte å fakturere i begynnelsen av juli, og så i løpet av det halve året fakturerte det vi skulle fakturert på et helt år. Og det var fantastisk godt å registrere at innbyggerne våre taklet å få mange fakturaer på kort tid. Vi var jo på tilbudssiden, vi var ute, og vi sa, og vi kommuniserte i alle kanaler, at hvis dette medfører problemer for deg så skal vi finne de løsningene sammen. Det hopet seg opp med papir, fordi der vi normalt har digital dokumentasjon, eller dokumentasjonen i digital form, så ble det papirbunker. Og mange plasser inneholdt de bunkene personsensitive data, og vi var nok ikke de beste i klassen på oss sikre fysisk de dataene. Så det var nok kontorer som ja, kontordøra var låst, men på en pult eller et skap, så var det i en periode personsensitive data tilgjengelig. Det gikk litt tid før vi fikk fokus på det, og den fikk også en dimensjon inn i det gjenoppbyggingsarbeidet vårt som vi kom i gang med forholdsvis tidlig, at av de 6 eller 7 temaer som vi hadde, så var personvernet en del av det. Men det gikk litt tid i starten der vi da ikke hadde gode rutiner for å sikre fysisk til personsensitive data, dette bør endres i et evt. nytt beredskapsplanverk.»

Personvernombud:

«Det er jo litt sånn kanskje man skulle skrive mer om, hva slags kompetanse en slik varslingsgruppe bør ha, altså de som skal være med der. Det er jo ikke sikkert at folk er her. Jeg har ikke spurt kommunedirektøren om akkurat det, for det jeg vet at han orienterer jo meg om når det er noe, og jeg stiller spørsmål, og fokuset har selvfølgelig vært her så langt gjenoppbygging, så jeg tenker at dette oppdraget ditt da vil vel danne grunnlag for hvordan man tar dette inn. Men jeg ser jo at i sånne settinger, så tenker jeg at personvernombudet hvert fall må involveres og ha en viktig rolle. Jeg kan jo spørre så mye jeg vil og er jo sånn sett underlagt taushetsplikt også i alle retninger, men det hender jo det at man kanskje skulle vært observatør da i noen møter for å snappe opp om det er noe som man skulle ta tak i på noe vis. Ombudet kan ikke være «hands-on» og det er de kjempeflinke med her, jeg følger jo mange andre kommuner rundt omkring, og jeg ser at når man lyser ut en stilling hvor man skal både være personvernombud og ansvar for informasjonssikkerhet og personvern da tenker jeg at da har man ikke skjønt ombudsrollen for å være helt ærlig. Nå har vi en databehandleravtale for å se at dette er greit, DPI-er begynner man å bli veldig god på, og der har jeg hatt observatør-rollen for å se om vi gjør dette på en god måte fremover nå. Det jeg mener er å presisere at ombudsrollen må adskilles fra det å ha ansvar for informasjonssikkerhet og personvernsikkerhet. Ombudet skal påse at GDPR

er ivaretatt. Da jeg har nevnt databehandleravtale er det for å gi et eksempel på at jeg noen ganger blir bedt om å lese igjennom databehandleravtaler for å sjekke om de kan aksepteres. Hver gang vi skal ha opp et nytt verktøy, så har jeg tillit til at det fungerer. Så ombudsrollen må folk skjønne hva en måte er, ja også ute i kommune-Norge. Det er ikke å sitte «hands-on» og gjøre ROSen og DPIene. For hvordan skal du skrive en uttalelse på det som du selv har vært med og gjort som ikke går i retning av det du har levert. Altså i forhold til datasikkerheten så er det jo sånn rent personlig så er det jo også min kompetanse fra før av, jeg har også utdanning på dette, men jeg har ikke brukt den til så mye for jeg synes ikke det var så morsomt, men at det er svært nødvendig med å ha fokus og sikkerhet på systemene det er helt klart. En ting er i forhold til rollen min her, at man har en forordning som man må forholde seg til, og det må man gjøre, og om man tenker at den er tilpasset norske forhold eller ikke det tenker jeg også er en greie. Vi gjorde det og må jeg si, vi gjorde jo noen vurderinger også i den gruppa på det. Det var blant annet lekket noen referat fra AMU (arbeidsmiljøutvalget), og der står det hvilke fagforeninger som er representert og med hvem, og vi vurderte eller jeg da at i Norge så er ikke det det har ikke noe med liv og død å gjøre. Hadde det vært i Polen for 30 år siden så hadde jeg nok sett helt annerledes på det, men forordningen er bærer preg av å være skrevet av jurister som ikke har ikke skandinavisk kultur da, så jeg skrev også noen vurderinger på det, at det det vi ser hvilken fagforening man er organisert, at det det har kommet ut, men det jeg tar vi ikke så alvorlig da. Så den det er det som går på den ombudsrollen hvor viktig det det er å ha sikkerhet rundt det, hvor viktig det er å ha altså lukkede systemer, og det er jo også viktig for kommunen, altså i forhold til omdømme og sånn, at man også er nøye med hvordan man håndterer møtereferat og sånn på altså folk som vil etablere seg, altså det er noe med omdømme og det er noen må også til dels en variant av bedriftshemmeligheter, selv om ikke vi har så mye av det. Og jeg tenker jo også beredskapsplaner, det har ikke noe med Østre Toten å gjøre, men jeg fant jo tilfeldig for noen år siden i en nabokommune hjemme hele beredskapsplan, altså hvilke hoteller vi skal evakuere til, hvem som har hvilke roller, hva man gjør her og der, reservevann løsninger og alt mulig sånt, og da ble jeg veldig overrasket. Så jeg mener også sånne ting også, og jeg tror også kommunen skal av beredskapshensyn vurdere veldig strengt i forhold til forvaltningsloven hva man egentlig faktisk skal bør kunne unnta offentlighet. Det er også en greie som jeg tenker på som bør være en del av det hele. Jeg tror at det er lurt å være litt strengere enn det man egentlig er i dag. Nå har jeg også i veldig mange år vært politiker i min hjemkommune, og nå sitter jeg i utvalg for plan og næring og der har vi jo en del av disse, vi har ikke beredskapsplanene men vi behandler jo mye, og det er mye saksdokumenter og som jeg tenker at om er det noen som har litt ugreie hensikter så er det bare å gå inn på møteplanene. Det er noe jeg har tenkt veldig på i etterkant, at hvordan håndterer man det? Så er det jo det at man blir jo lammet da, jeg er jo glad når jeg begynte her at jeg også var på tråtT i 86, så jeg visste at jeg kan gjøre mye med penn og papir. Men så er det jo da etterpå, å holde orden på dette her, sørge for at ting som kommer inn er lagret, det som er arkivverdig skal ligge her og det skal ligge der.»

Fylkesberedskapssjef:

> «Vi lærte nok mest at dette her kan skje da, og vi hadde jo teoretisert litt rundt det på forhånd, og så videre, men at det faktisk skjedde på den måten var jo en vekker. Statsforvaler eller den gang Fylkesmannen hadde jo selv blitt hacket i 2018, så vi visste jo at det her kunne skje, men at det ble så omfattende i kommunen det var jo en overraskelse egentlig. Det var vel i hvert fall en oppvåkning, og når vi nå forbereder kommunen på noe sånt i ettertid, så er det veldig nyttig å ha Østre Toten hendelsen i bakhånd slik at du vet hva som er realistisk scenario og det er faktisk det her.»

Sikkerhetsekspert ATEA:

> «Man kan lære av hva det er å ikke gi bort for mye detaljer til pressen. Være åpen og ærlig, men heller ikke gi alle detaljer ut fordi det reagerte jeg på da, då jeg plutselig så pressemeldingen som gikk. Det å ikke kunne kontrollere informasjon som gikk ut fra hendelsen, da kommunikasjonsavdelingen ikke kunne håndtere informasjonen, så presse fikk jo fri tilgang til å intervjue sykehjemsleder og andre kommuneansatte og sånt noe, og det er jo ikke sånn IT-sikkerhetsmessig så veldig bra da. Når du gir informasjon så vet du ikke hvilke andre som hører på på en måte. Så det så det var jo en del av saken.»

*Hva slags form for beredskapsplaner eller tiltakskort ble benyttet ift. ditt arbeid i krisehåndteringen?*

Ifølge ordfører har det tidligere blitt gjennomført arbeid rundt beredskapsplanverk med tidligere rådmann, hvor beredskapsplaner ble vedtatt. Dette var imidlertid noen år tilbake, og etter det har det ikke vært oppe i kommunestyret. De hadde noen planer som de tok frem, men ordfører var usikker på hvor brukbare de var i praksis var for kriseledelsen.

I helse og omsorg er det beredskapsplaner, men det er ikke pekt på spesielt en cyberhendelse, men det kan være strømbortfall eller at systemer faller ned, noe det ifølge helse- og omsorgssjef har vært bevissthet rundt. Og at det da har vært en minimumsløsning for beredskap for det å få tak i opplysninger. Hun beskriver at dette i hovedsak har dreid seg om fagsystemet, da man har hatt en opplevelse av at dette systemet kan være ustabilt. Dermed har dette vært fulgt opp, og man har hatt beredskapsplaner for å håndtere slike situasjoner. Hun mener allikevel at det kan være et stykke ifra det man sier man skal gjøre til etterlevelse, men at det var veldig heldig at de i den fasen hadde tilgang på de aller nødvendigste data.

Ifølge økonomisjef forholdt de seg i utgangspunktet til den overordnede beredskapsplanen, selv om de har en stabsfunksjon, men det var mye de opplevde som ikke var tenkt på. Beredskapsplanen i Østre Toten kommune hadde ikke tatt høyde for at de skulle utsatt for det de ble utsatt for.

> «Vi har litt om flom og flyulykker og kanskje også alvorlige ulykker ellers, streik og sånn, men at vi skulle bli satt tilbake til penn og papir på syttitallet, det har vi jo nok ikke planlagt noe særlig. Ja, så det er jo også et læringspunkt her, at den situasjonen kan oppstå.»

Personvernombud hadde ikke sett på det, men i kvalitetssystemet så ligger det ifølge henne en god del beredskapsinformasjon. Hennes rolle er imidlertid ikke så godt beskrevet, men det er godt lagt til rette for at når man varsler avvik hvor det kan være aktuelt å få en uttalelse fra personvernombudet, så har det ligget der også før, og det er ifølge henne utvidet.

> «Så det avvikssystemet vårt det synes jeg er bra, og jeg opplever at det fungerer når man først melder. Men hvor god man er til å melde, det generelt er nok en diskusjon. Så det å melde avvik det kan man nok med fordel gjøre mer av, men jeg tror at den kulturen er litt å jobbe med. Man melder på store ting, og jeg kan ikke si at jeg har hørt avvik som går i forhold til personvern som ikke er meldt, det har jeg ikke. Informasjonssikkerhetsavvik har jeg ikke sett noe til, men vet at det snakkes om det, det er jo snakk om animasjoner og litt sånn forskjellig. Men det bare hører jeg at det er det snakk om. Og det er også gjennom at jeg har overvært noen arbeidsmiljøutvalgmøter. Og der er det jo også et hierarki, for dette er sorterer jo også under helse, miljø og sikkerhet faktisk. Vi får stadig påminnelser, sånn husk ditten og husk datten, men hvor effektivt det er å bruke dette første skjermbildet som jeg kaller det, litt usikker på det. Så det kan det nok med fordel gjøres noe mer. Men tankene er der, men jeg kan ikke med hånden på hjertet si at det er noe alle har fått med seg og tar inn over seg, for det er å ta det inn over seg som er det viktigste.»

Hos Statsforvalteren har de tiltakskort ved bortfall av ekom og strøm som det går an å benytte seg av, og fokuset er på konsekvensen av denne type hendelser.

Sikkerhetskonsulenten fra ATEA mener man bør i skille på en vanlig hendelse og en sikkerhetshendelse. Det jo mange typer sikkerhetshendelser og det ATEA har gjort er å lage senario-bøker for alle typer hendelser, eller som han sier: «de mest vanlige «incidentene» da, som vi er borte i».

> «Sånn som de har lagt det opp i forsvarssektoren da, så har de først en overordnet sikkerhetsleder, og så har de en datasikkerhetsleder som har hele stemme og så har de da en «incident «manager, sistnevnte gjerne lokalisert sammen med datasikkerhetsleder i IT-avdelingen eller i hvert fall under IT-direktøren, hvor de da har litt forskjellige roller i en «incident» hvor dataleder rapporterer i myndigheter og sånt, noe mens «incident» manager holder i trådene rent IT-messig og «forensics»-messig da. Må prøve å ha den oppgaven jeg hadde da, i Østre Toten, og da med hjelp av eksperter, hjelpe kriseteam med å rapporter på hvor langt vi er kommet i forskjellige saker.»

*Hvilke anbefalinger vil du gi til kommuner og andre organisasjoner?*

Ordfører:

> «I den rapporten som kom og er skrevet av KPMG i forbindelse med vår hendelse så var det jo sånn at han som hadde ansvaret for sikkerheten i kommunen, altså rapporteringen til kommunedirektøren var det nok så som så med på sikkerhetsområdet. Vi leste det i KPMG-rapporten og at det kanskje ikke var så vits i å rapportere oppover heller for det var ikke politisk vilje til å

dele ut mer ressurser til dette området til sikkerhetsområdet med hensyn på data. Så var det jo sånn at den nye rådmannen bestilte jo informasjon om dette før dataangrepet, så jeg tror kanskje det kunne skjedd noe der, men mitt råd er jo at politikere etterspør sånn rapporter oppover i systemet, altså rapporteringer fra dem som er sikkerhetsansvarlige, at det kommer til kommunedirektøren og videre til kommunestyret sånn at man blir klar over hvordan situasjonen er. Først så må du vite hvordan det står til, og når rapporteringssystemet fungerer, og når du får vite hvordan det står til så får du muligheten til å agere ikke sant. Om du velger å ikke gjøre det da, men da er det på en måte din egen skyld da. Det første som alle bør være interessert i, det er det her å få rapporteringsrutiner til å fungere sånn at kommunestyret er klar over hvordan situasjonen er, hvordan risikoen er og hvordan det blir håndtert i den enkelte kommune. Min klare anbefaling er at man gjør det først og så er det sikkert mange forskjellige ting en kan gjøre for å få vite hvordan det står til. Hvis man ikke vet hvordan det står til så får man i alle fall ikke gjort noe.  Det er viktig å ha en leder i kriseledelsen, hvis det er en spesiell situasjon sånn som det her på et på et visst fagfelt, så er det nok viktig å ha en ledelse som forstår problemet da. Det hadde jo vi i dette tilfellet her, og da kan vi følge egentlig den organisasjonsmodellen som vi har. Fra kommunedirektøren og utover i sektorene. Så er det nok viktig når det blir sånn spesielt som dette her, jeg opplever at en liten del av en kommune, som var en veldig viktig del en grunnleggende del ikke sant, så er det viktig å få tak i noen eksterne som kan gi råd da, på et tidlig tidspunkt, og at du klarer å finne ut en 2, 3 forskjellige aktører som du kan få råd ifra, sånn at det blir litt lettere gjøre de riktige tingene. Råd fra han fra KS på det strategiske valget i oppstarten, det tror jeg var viktig for oss da. Ja, de hjalp oss fra KPMG og andre, men på det strategiske gjenopptaket tror jeg han fra KS hadde mye å si for hvordan vi skulle ta oss opp igjen. Og hvilken strategi vi skal velge da. Vi var jo lenge inne på tanken om å ta oss opp sånn som vi på en måte var da, gjøre alt dette på egen kjøl, så det gikk en stund før vi innså at det ble for vanskelig da. Da tror jeg han fra KS var en viktig rådgiver i så måte. Så jeg tror det er lurt at en organisasjon som KS som er kommunen sin egen organisasjon og overordnede paraplyorganisasjon har noen ressurser som kan som kan gå inn i flere lignende organisasjoner og hjelpe til når det er spesifikke sånne kriser og problemer. Når det gjelder strategisk planlegging tror jeg det er lurt. I kriseledelsen så opplever jeg at beslutningene ble tatt i tråd med den organisasjonsplanen vi har, så det fungerte det.»

Kommunedirektør anbefaler først og fremst å følge NSM sine grunnprinsipper med hensyn til sikkerhetsstyring og drift av IKT kommunens IKT systemer. Han anbefaler også å planlegge for bortfall at flere IKT systemer samtidig, og å lage nødprosedyrer for bortfall av IKT systemer og ikke minst lage beredskapsplaner.

Kommunalsjef helse og omsorg:

«Jeg tror det er viktig å ha beredskapssystemene i orden på det området her og, på lik linje med andre områder. Og det tror jeg har vært felles for mange norske kommuner, man har hatt fokus på skoleterror og sånne ting, som det kanskje er veldig mye lavere sannsynlighet at kommer til å skje, så det å innarbeide det i det ordinære beredskapsarbeidet, og ha orden i sysakene

sine og orden i eget hus, og det er jo det vi driver med nå, det er jo det å få opp rutinebeskrivelser, få opp varslingssystemer, hvem er det som skal ha beskjed, hva betyr dette her, og så må vi gjøre en vurdering og fordi det er jo klart økt sikkerhet gjør jo noe med både tilgjengelighet og funksjonalitet, det kan virke begrensende, og det er jo kvalifiserte valg som kommunen også må gjøre. Hva slags risiko er akseptabel å leve med? For sånn er det jo på alle andre områder også. Sånn sett skiller jo ikke dette seg nevneverdig ut. Men for mange av oss så blir dette her veldig ukjent terreng, ikke sant, mye av dette er jo begrepsbruk og språkbruk som vi og menigmann ikke forstår. Det blir veldig teknisk en del av det. Det er viktig å «tilgjengeliggjøre» det. Språk som gjør at folk forstår hva dette dreier seg om. Noe av dette har jo utviklet seg i en retning, som vi på en måte har akseptert, med mere deling på grunn av digitaliseringen. Og det er jo selvfølgelig noe av gevinsten også, men så må man jo da ta med seg ulempene, og et eksempel er jo det med kjernejournal, før så var det på papir, da måtte man be om å få det oversendt, eller si at det skal sendes hit og dit. Nå ligger det jo tilgjengelig for alle de som har tilgang på kjernejournalen. Det er jo ikke nødvendigvis slik at pasienten ønsker at alt det som står der, at alle skal vite det, men det ligger der det. Framtida vil sikkert også være slik at også pasienten får hånd om sin egen informasjon. Og at man kan gradere det i større grad enn sånn som det er nå. For jeg tenker at om jeg går til øyenlegen så har ikke den øyenlegen brukt for informasjon fra kjernejournalen som angår mitt underliv. Jeg syns egentlig det er gode eksempler. Og det er jo gevinster som alle heier på at vi skal få, men som ikke er nødvendig for alle å få. Og hvis jeg skulle velge å gå å kjøpe meg en privat helsetjeneste, så er det jo ikke sikkert at jeg ønsker at fastlegen min skal vite det. Så jeg har delte synspunkter om det med en journal. Det er ikke bare udelt positivt. Det som er en utfordring når du får en så massiv hendelse som vi hadde da, så er det det å få en god samordning på tvers, vi etablerte ganske raskt en god kriseorganisasjon, og vi har en kommunedirektør som er veldig god på informasjonshåndteringa, og som hadde en veldig bevisst tanke omkring at vi skulle være åpne. Og det tror jeg har vært kjempebra, og viktig, og det tror jeg Østre Toten har stått seg gått på, å være åpne på det som har skjedd. Men sånn vil det alltid være tror jeg, det å gå ut med informasjon, og det å få sikret at det er en god samordning. Det var hyggelige møter og jeg opplevde at det var veldig bra. Kan ikke si nå at det er noe som skulle vært annerledes akkurat i krisehåndteringa. Bortsett fra det jeg sa i sted, vi strevde i starten med å få god nok oversikt og det henger jo sammen med det vi snakker om nå, å ha god nok samordning da. Men sånn tror jeg det ofte er i oppstarten av kriser, sånn var det med corona og, det er litt krevende inntil man finner formen.»

Økonomisjef:

«For det første så håper jeg at ingen opplever det vi opplevde, jeg unner ingen det. En ting er selve hendelsen, det andre er hvordan dette påvirket oss i organisasjon, og tok all fokus. Vi som hadde mange planer og som hadde mange oppdrag i fra folkevalgte i kommunestyret, vi hadde jo nylig vedtatt et budsjett, og i det budsjettet så er det mange ting som vi har fått beskjed om å gjennomføre, og så må du sette mer eller mindre alt til side. Spesielt sett i fra mitt ståsted, som er en del av denne stabsstøtte funksjonen, ikke sant, vi skal

jo på en måte hjelpe alle til å bistå, legge forholdene til rette, vi skal hjelpe til med rapportering, og vi skal søke, og så videre… Den følelsen av å ikke kunne levere samtidig som over tid så jobber du så intenst, du jobber på adrenalin, så ser vi at det sniker seg inn slitasje. Og det er nok en ting som vi må trekke litt lærdom av at må observere hvordan det går med folka i organisasjonen. Er du ansvarlig leder så kan du hende at du takler det, men det er ikke dermed sagt at alle dine folk takler det på samme måten som deg. Det er noe som jeg kjent på litt i ettertid, at vi kunne med fordel ha vært mer observante og fanget opp slitasje. Jeg tror faktisk at det at noen med fordel kunne ha fått litt oppmerksomhet i den situasjonen de satt i, og blitt spurt hvordan det går, ikke bare forvente at det skal gå. Vi levde jo med denne datakrisen i tilnærmet ett år, vi sa jo at vi var i tilbake i tilnærmet normal drift i midten av november, det hadde gått 10 måneder, men vi var det egentlig ikke. Enda så er det en del som er berørt. Men dette her med, vi er i en middels stor norsk kommune, vi har de folka vi har og oftest så er det post type spesialistfunksjoner, veldig få, slik at vi satte jo sammen de beste folkene våre til å jobbe med, på en måte, denne gjenoppbyggingen, og det var på en måte ikke bærende å så gå ut og rullere og hente inn nye folk. Jeg tror at det er 2 ting, det ene er den observasjonen å prøve å fange opp hvor den er den slitasjen, og kanskje også å forebygge ved å sikre at noen får en liten pause. Jeg tror at vi vi hadde, altså helt rett i starten, så var det nesten 24/7 og da hadde vi noen fysiske pauser. Det var på selve hendelseshåndteringen, og når den første helgen var ferdig så måtte folk få lov til å komme opp på jobb på mandag klokka 10.00 i stedet for klokka 06.30. Vi måtte jo bygge en type organisering av alt dette, og alt dette er jo da både å finne ut hva det var som skjedde, hvordan skal vi forklare hva som skjedde, årsaken til at det skjedde, og hvordan skal vi bygge opp igjen punkt 1) den infrastrukturen som var nede og alle fagsystemet som vi fant ut etter hvert måtte bygges opp på nytt. Og, så dels brukte vi de samme folka på begge deler, og så fant vi ut at ja det var kanskje ikke det aller lureste, så vi endrer jo denne prosjektorganisasjonen vår litt underveis, ved å si at ja nå jobber du med infrastruktur, så jobber du med fagsystemer, men så gikk det ei tid, og så fant vi ut at nei nå på dette stadiet så ser vi alt under ett. Så vi endret jo både noe på folk, men også noe på måten vi jobber på. Og så trekker vi inn sånne såkalte perifere, ikke sant, ikke bare de harde tingene, men trekker dette med personvern og informasjonssikkerhet, den dimensjonen, inn i dette arbeidet. Og også kommunikasjonsdelen da. Vi brukte ikke mye tid på å finne ut at kommunikasjonen var viktig, men vi vi brakte kommunikasjon på banen med en gang. Så det jo en strategisk ledelsesbeslutning, at vi skulle være åpne, både internt og eksternt. Så vi var ekstremt åpne om dette hele tiden.»

Personvernombud:

«I hvert fall det å ha tenkt igjennom å ha, for det er jo det er jo særlig det med varsling som er viktig i forhold til forordningen, og at man har tenkt igjennom for det første hvem som kan være aktuelle eller hva slags kompetanse det er lurt å sette sammen. Så tenker jeg det er lurt der man har mulighet for å få vite og få hjelp til å gjennomgå informasjonen som er lekket, at en sånn type maskinell analyse i første runde, med at det er lurt å ha forvisset seg om - hvor kan vi kjapt få tak i det og få nødvendig hjelp til det. Så tenker jeg jo at det er

veldig viktig for hver eneste organisasjon å vite hva slags informasjon har de lagret. For kommune Norge så er det fra før fødsel til du er under oppløsning, så det tenker jeg der er det jo kjempeviktig. Men det betyr jo ikke at jeg tenker at alle organisasjoner er der, men det er klart at hvis vi skal se på mye, altså Mattilsynet har jo enormt med bare for å ta noen sånne ting som jeg kjenner til, informasjon som er superviktig og som kan også berøre noen, og fylkeskommunen har jo også mye på helse. Jeg gikk jo veldig fort telefon fra Nordland, så jeg har jo fått en god venninne der for å si det sånn. Hvor vi har bistått med alt (delt vurderinger og hvordan vi jobbet Østre Toten ble angrepet). De få henvendelser vi har fått, der vet jeg både kommunedirektøren har bistått enormt og jeg har gjort det, bare anonymisert våre vurderinger og stappet det ut, for å si det sånn. Så det å ha kontroll på hva slags type informasjon man har, som er innenfor de gruppene som er dekket av forordningen, det er i hvert fall viktig på personvern. Fordi at hvis du vet at det er en liten del som er stjålet og lekket og den lille biten ikke inneholder noe så er det jo egentlig ikke et stort problem. Så det er jo noe med å maksimere eller minimere her. Så det er et råd jeg ville ha har gitt. Og så har vel jeg opplevelsen av det er nok litt forskjellig da, men det er nok ikke alle ledere som er helt klare på personvernombudet rolle, og det er litt fordi at det har jo vært jeg har jo blitt kontaktet et par som har hatt noen utfordringer, hvor de på en måte ikke får bli med, og ikke blir delaktig fordi at man tenker ikke at det er en greie.»

Innsatsleder IKT:

«Skal jeg være helt kald og konkret, så må jo det være å være forberedt, og du må tenke beredskap også på det her området, ikke bare på de tradisjonelle områdene (der vi har beredskapsplaner). Det du trenger i en sånn setting er gode venner, og hvis du ikke har en plan og ikke har noen tanker om hvem som kan hjelpe deg, så blir det jævla tøft. Det er kanskje feil rekkefølge å bare starte med beredskapsplaner, man burde også begynne med å sikre seg selvfølgelig, mot sånne hendelser. Mine tips vil være å faktisk ha fokus på å sette av midler og bruke penger på riktige sikringstiltak. Og det er jo både tekniske sikringstiltak og alt mulig av teknologi som sikrer deg, men også det å styrke menneska oppi det hele da, som er en stor del av at det skal unngå at det skal skje med å styrke kompetansen der. Men tilbake til det med planer, der må jo tipset være at parallelt med at du sikrer deg teknisk, så du har en plan for hva du gjør når det skjer, og å ha avtaler med partnere som kan hjelpe deg, slik at du har kontaktinformasjon, navn, hoder, ansikter på plass når det smeller, og du må begynne å jobbe.»

Fylkesberedskapssjef:

«Ja det må jo være for det første å ha ting gjennomtenkt rett og slett, beredskaps planer er jo det viktigste man har da, men beredskapsplaner kan jo fort bli litt teoretisk, så man må jo slett tenke gjennom og kartlegge kanskje, hvis nå ting skulle bli borte, hvilke systemer blir borte, hvilke henger sammen som er avhengig av hverandre. Ser sånn som i Østre Toten er går noen systemer på egen kjøl, mens andre er avhengig av hverandre. Noen hadde de felles med Gjøvik, og de fungerte jo. CIM fungerer for eksempel. At man ikke

blir overrasket hvis man får et løsepengevirus, om hva som forsvinner, tror jeg er viktig. Og at man har lite-granne back-up planer og kanskje har beredskapsplaner skrevet ut på papir. Det du ikke har gjort på forhånd får du nå i hvert fall ikke gjort når det skjer tenker jeg. Altså hva er det som er spesielt med cyber-sikkerhetshendelser, en kommunedirektør er fortsatt en kommunedirektør så det er jo ikke noe å lure på. Vi anbefaler at en cyber-hendelse er som en hvilken som helst annen hendelse, så man må bruke de systemene man har. Det som jeg opplevde med Østre Toten, som jeg syns de gjorde bra, var de rigga jo to linjer med en gang. Den ene var en standard beredskapslinje, ikke sant og hvordan håndterer vi konsekvensene av dette her, og det er jo felles for alle beredskapshendelser. Den andre linja var jo den tekniske linja at man begynte å se etter hvordan man kan håndtere det tekniske aspektet da. Rense, bygge opp igjen på nytt osv osv. Som da ble ressurssatt med blant annet ATEA og KPMG og de folka der da etter hvert. Det synes jeg var bra de hadde de hadde et veldig bevisst forhold til hvilke konsekvenser fikk denne hendelsen som man måtte ordne opp i, altså blant annet dette med manglende etter-kriser på hendelsen for eksempel som er en konsekvens av en sånn hendelse. Så jeg tenker jo det at jo mer jo mer likt man klarer å håndtere konsekvensene med andre typer hendelser som man har øvd på, jo bedre er det. Da er man trygg i det man skal gjøre.»

Sikkerhetskonsulent ATEA:

«Så lenge du har en varslingstjeneste som fungerer, de skal jo ikke varsles om alt, men varslingstjeneste er jo at man får veldig mange varsler ikke sant, så det må jo kategoriseres etter kritikalitet, og det som oftest skorter på det da er jo når noen blir ringt opp, hvilke rutiner er det som ligger der, er det å ringe IT-sjefen og gjenoppbyggingsansvarlig og be dem etterforske pent, eller hvilke rutiner liker liksom bak der. Og så er det jo da å få eskalert riktig sånn at man får prioritert sakene riktig og bare når det er noen virkelig faktisk som ikke kan gjøre dette selv ikke sant. Så snart kommunen kan ta en beslutning når ting skjer, altså disse direktørene vil jo ikke bli ringt opp for all verdens ting ikke sant, så det er det er det å få finne den der balansen mellom det som er kritisk og det som ikke er kritisk, og hvor de rutinene som ligger bak der igjen da, hvilke beslutningsprosesser som gjøres snart virkelig er kritisk. Så er det jo det da, har du har vært utsatt for et sånt opplegg, velger man da å stenge ned hele kommunen for den minste ting eller har man et har man et edruelig forhold til det, det er også en greie da. Hvor gode rådgivere har de hos IKOMM eller hos andre, eller internt, for å for å ta de riktige beslutningene. For det første må du jo ha den riktige informasjonen til å ta beslutninger på og det innebærer jo at da de som sitter på den SOC-en klarer å være nok da, til å gi riktig informasjon. Vår egen SOC kontakter jo IRT når de lurer på noe, og vi ser jo at vi er hindrer en del falske meldinger til kunden fordi vi tar en edruelig beslutning på at nei dette ser ut som at det en «VPN som er nede», her må vi undersøke litt nærmere før vi kontakter kunden liksom. Det vi ser er at alle disse sårbarhetene blir utnyttet av kryptominere først, og så når de får tenkt seg litt opp så kommer da randsomware-bølgen eller APT-ene.»

*Hvilke anbefalinger vil du gi til arbeidet med roller i krisehåndtering?*

Kommunalsjef helse og omsorg:

> «Vi hadde jo etablert en struktur for at det var jo corona samtidig, så vi har nesten gjennom hele coronaen hatt ukentlig beredskapsmøter i sektoren, med alle lederne og ressurspersoner, og det har også vært tilgjengelig personer utenfor sektoren, altså renholdsleder, leder for vaktmesterne, fra bygg og eiendom som har vært med i det beredskapsmøtet. Så vi brukte jo det møtet og vi samla jo alle lederne + lederne i stab i dette møtet den lørdagen, og så fortsatte jo hendelseshåndteringen som en del av det beredskapsarbeidet vi allerede var i gang med. Så det å etablere en egen beredskapshåndtering i sektoren var ikke vanskelig, for den var allerede tilgjengelig. Og ganske tidlig også så dedikerte vi, vi har en stabsressurs, en fagrådgiver som har videreutdanning i beredskap, så han var jo ferdig med det da, og tok en aktiv rolle i å koordinere og håndtere noen av de tingene som måtte sentraliseres. Det er jo andre problemstillinger enn det det er i andre deler av kommuneorganisasjonen med tanke på det som går på digitale arbeidsplater og sånne ting. Det er stort strekk i laget på hvordan den digitale kompetansen er. Og bare det å kunne komme ut med beskjed til alle ansatte, er en kjempegreie, og spesielt når alt er utilgjengelig. Så han tok en veldig aktiv rolle, for å koordinere og følge opp, og det fungerte veldig bra innledningsvis, til vi hadde klart å komme mer over på et driftsspor egentlig. En stor utfordring i starten, det var at dette var relativt uoversiktlig i en tid, det er jo litt vanskelig å huske hvor lang tid, og mange prosesser var jo ikke jeg involvert i. Her er det jo mange fasetter, du har jo etterforskningssporet, du har gjenopprettingssporet, du har krisehåndteringssporet, du har informasjonsbehovet, det er mange fasetter da, som skulle håndteres. Og veldig mange av de var jo ikke vi sektorlederne involvert i, det ble jo håndtert av kommunedirektøren, kanskje alene da, opp imot politi. Opp imot sikkerhetsmyndigheter og den slags, og der var det jo sikkert konfidensielle opplysninger som ikke alle skal vite, og så det var ganske uoversiktlig i starten, og da hadde man fokus på at dette må vi bare få opp igjen. Og da gikk jo det til et punkt hvor det ikke gikk lenger, og da ble det tatt noen beslutninger som ga føringer for den videre oppfølginga. Så det er vel det jeg sitter igjen med litt, at veldig mye har kommunedirektøren håndtert sjøl opp imot de ressursene som har vært både eksternt og internt. Nesten en litt sånn task force gruppe da. Som har jobba med det. Det har vært greit for oss det, og vi har fått den informasjonen vi har hatt behov for, og så ligger det mye mer der, det veit jo jeg og, men av helt åpenbare årsaker så skal ikke det spres på flere enn strengt nødvendig.»

Økonomisjef:

> «Altså kriseledelsen vår er ganske bred bredt sammensatt og vi snevrer ikke den inn fordi at det var data og ulykke eller pandemi. De samme folkene var jo i kriseledelsen, så kommuneoverlegen var jo med når vi hadde kriseledelse om datainnbruddet. Så vi fikk jo med oss de her dimensjonene på hva gjør en krise med en organisasjon og for folk. Så egentlig så ivaretok vi det underveis, og så supplerte vi kriseledelsen med IKT delen, slik at IKT-sjefen kom inn, og

vi hadde vi hadde beredskapslederen hos statsforvalteren med oss i møter i kriseledelsen i starten, vi hadde kommune-CSIRT på banen som også deltok i møter med i kriseledelsen. Vi hadde en kriseledelse som behandlet datainnbruddet i utgangspunktet som en hvilken som helst krise, men som jeg har sagt litt tidligere, det var nok noen sånne elementer i dette som tok litt tid før det sank innover oss at det var viktig å ta på alvor. Og det var da med personvernet spesielt, og den sikringen av det, men også den med slitasje. Vi har vært åpne om det, og sagt det, skrevet rapporter, og i årsrapporten vår nå så vil det stå noe også om dette - at vi har en organisasjon som i løpet av året var preget av, og ikke bare en slitasje, men frustrasjon fordi at folk ikke får gjort jobben sin. Folk ble utålmodige, og så ble det gjort en forholdsvis tidlig prioritering av hvilke datasystemer som skulle prioriteres. Vi laget et såkalt bruttoliste: Den listen innhold i starten 240 systemer og system avhengigheter, for det er integrasjon nesten «all over», ikke sant. Så sa vi at liv og helse har prioritert nummer én, miljø nummer 2 og så får økonomien og alt det andre komme etterpå. Då det er klart at i dette bildet her, så er det noen som jobber med ting som da er viktig for dem og for det området de har et ansvar for, og så er det langt ned på prioriteringslista. Det var ikke utfordrende å informere om det, men det var kanskje utfordrende å registrere den frustrasjonen som det medførte i organisasjonen. Så kombinert med at folk måtte jobbe tungvint og ikke fikk utført jobben sin, og mange identifiserer seg med at de som skal nyte godt av det er den jobben de produserer, enten det er innbyggere, eller brukere, eller hva som helst, så blir de frustrerte på deres vegne. Fordi vi ikke blir i stand til, selv om vi klarte veldig mye i den perioden. Vi doblet i hvert fall kapasiteten med informasjon. Vi hanket jo inn folk som vi mente var gode på informasjon, og sa at nå er det informasjon du skal jobbe med, for det andre får vi tatt igjen en gang. Også på dette feltet her da, kommunikasjon og informasjon, så skulle vi håndtere dette parallelt med at vi hadde en koronasituasjon som også var en krise. … Hjemmesiden vår kom jo opp igjen forholdsvis tidlig og den ble jo også informasjonskanalen internt i organisasjonen. Og når vi skulle informere våre 1300 ansatte, så var det en type informasjon som også var åpent tilgjengelig for alle. For det var jo ikke et intranett vi snakker om nå, vi snakker om at vi brukte kommunens hjemmeside til å informere våre ansatte.»

Personvernombud:

«Nå tenker du Grethe på hvem som er ridder av det runde bord? Personvernet er også uavhengig av om det er informasjonssikkerhet eller ikke, personvern handler også om du er litt uheldig og har pcen din stående, altså det er mange ting, og man kan ha et ulåst kontor og det er papir som flyter. Så jeg tenker at personvernbiten er viktig egentlig uansett, ikke bare ved et cyberangrep da. Jeg har jo, eller personvernombudet har jo, en selvstendig forpliktelse til å stille spørsmål. Men det er klart at da må man jo virkelig sette seg inn i rollen og det skal jeg være ærlig å si, at hvis ikke dette hadde skjedd, så ville jeg nok selvfølgelig ha skummet GDPR og sånn, det ville jeg gjort, men jeg hadde jo aldri brukt (når jeg har 20% stilling), så hadde jeg aldri brukt så mye tid som jeg brukte på å være sikker på rollen min. For jeg sto jo litt alene (det er jo bare et personvernombud), altså du må ha du må jo ha integritet da, til å både stå imot det før du skriver, jo du kan jo også risikere å skrive inn uttalelser her

som er stikk i strid med det du vet at kommuneledelsen ønsker. For det kan ha en kostnadseskalerende side for eksempel. Så jeg tenker at det er viktig hva slags person som får en ombudsrolle, det er viktig. Og at jeg har vel lært at det å skolere seg, det må man faktisk gjøre selv altså. Så man bør ta kontakt med de nettverkene som er og jevnlig stille opp og følge med på det som foregår. Og da har man egentlig i den ombudsrollen, så har man et ansvar for også å stille spørsmål. Jeg vet ikke hvor ofte man har møter i kriseledelsen her, men jeg tipper at det er berammet og så avlyser man hvis det ikke er noe. Så er det klart at det kan hende at man burde fått være med som observatør når det når det er saker som tenderer da mot personvern, uansett om det er cyber eller om det er andre hendelser. Eksempelvis et innbrudd et sted hvor ansvarlig leder ikke er helt sikker på om dokumenter med sensitiv informasjon har ligget innelåst. Det er også noe med at selv om skapet er låst og du har gjort alt du skal og hele skapet er stjålet, da er det informasjon på avveie det må vurderes om det varsles. Jeg er ikke kjent med at vi har gjennomgått kan du si og kategorisert typer av informasjon som kommunen lagrer om noen som er rød, gul eller grønn. Man bør ikke gjøre alt, så det er ikke alt som bør gjøres så innmari stort, altså det er mulig å gjøre mye det er vi kanskje ikke like flink til. Vi skal ha store prosjekter og piloter og oldemora på alt. Det er noen ting som egentlig bare er å gjøre.»

Innsatsleder IKT:

«Når jeg satt der i den settingen, så satt jeg egentlig og drømte om at det skulle komme en slags sånn «cyber-swat-team» og bare komme med to store svarte lastebiler med mett med folk i og bare løse problemet. Det er spøkete sagt, men det er en viss sannhet i det, for det du trenger er folk som kan å navigere dette landskapet. Både på det organisatoriske med å koordinere mot de statlige instansene vi har som bryr seg om dette her, og det fikk vi god hjelp til med henne fra KPMG, som har jobbet i dette miljøet i årevis. Men du trenger jo det samme på teknologi. Dette her har skjedd, hva skal vi nå gjøre? Og det er jo egentlig et stort læringspunkt oppe i dette her, vi brukte jo 3,5 – 4 uker på å bygge opp igjen infrastruktur, som deretter ble skrotet når vi gikk til IKOMM. De 4 ukene var 100% bortkastet ift. den innsatsen som ble gjort på infrastruktur-siden. Og det var en konsekvens av at disse gode hjelperne våre pirket meg på skulderen en fredag og sa at dette vi gjør nå, dette som vi bygger opp igjen – infrastrukturen, det blir ikke bra nok, og dere kommer ikke til å klare å holde det på et nivå som er noe bedre enn det dere hadde før. «Dere mangler teknologien, og dere mangler kompetansen, her bør vi se på alternativer.» Det var rett og slett starten på en annerkjennelse som ikke alle er enig i, men i alle fall gikk den veien at IT-miljøet i kommunen var for dårlig både før, og vi så at vi klarte ikke å få det bra nok, sjøl om vi åpenbart hadde sikkerhet i fokus når vi bygde opp igjen infrastruktur. Og endte da opp med å gå til IKOMM, så den innsatsen over de 4 ukene på teknologi og infrastruktur ble skrotet, og så begynte vi helt på nytt igjen, men da med IKOMM. Alle som jobbet på IT-avdelingen ble overført til IKOMM, det som skjedde etter den verste akuttfasen, og etter at IKOMM hadde begynt å bygge opp igjen infrastrukturen. Selv fortsatte jeg i den her rollen som innsatsleder, men så fikk jeg et annet jobbtilbud som ikke har noe med hverken Østre Toten eller IKOMM å gjøre.»

*Hvilke anbefalinger vil du gi til arbeidet med opplæring, trening og øvelser?*

Ordfører peker på viktigheten av gjennomføring av øvelser i seg selv og nevnte at det ikke er så ofte de har det på forskjellige områder. Han mener at å sette opp «case» der man får et reellt problem slik man kan se at i den organisasjonen det er satt opp for, så kan det være forskjellig for en hendelse for en del av en sektor, men at du kan få noen øvet noen beslutningslinjer. Samt at man kan og ha en leder og en organisasjon som bruker det og får satt opp sånne øvelser.

> «Jeg tror ikke det er mange ordførere som har hatt flere krisemøter enn meg.»

Han mener derfor at det å ha realistiske øvelser litt oftere er viktig, at man ikke gjør det for vanskelig, og at man har det av og til. Han mener også at det å øve på å rapportere oppover i systemet på forskjellige ting, ikke bare på sikkerhet og på IKT, men også når det gjelder helsetjenester, sørge for at både varslingsrutiner og statusrapporteringer går som de skal, slik at man får vite oppover i systemet hvordan ting står til på en sektor.

> «For vi ser vi jo om du ikke gjør det, så kan det surre og gå i flere år, og når det først blir trøbbel da så, så blir det mye trøbbel, og da tenker jeg kan være lurt å etablere rutiner for å få statusrapporter fra forskjellige deler av den virksomheten som du har. Kanskje det viktigste er at du ikke lurer deg til å tro at det står bra til fordi du ikke hører noe. Man bør kanskje bli flinkere til å ha statusmøter for å få rapporteringer oppover i systemet. Hvis det blir en litt friere flyt av rapportering oppover i organisasjonen, så tror jeg det blir en sunnere organisasjon da.»

Kommunedirektør mener at det å være forberedt på at slike ting kan skje er viktig å øve på. Han kjenner kommunesektoren godt, og har vær med på en del digitalisering, og visste jo det at man kunne få utfallet av enkeltsystemer, men at det kunne få så store konsekvenser, var han ikke klar over.

> «At det var på en måte ikke så usannsynlig da - så man må lære det. Det er vel kanskje noe man tenker seg at det er ting som kan skje ikke sant…»

Kommunalsjef helse og omsorg mente det er viktig å øve på denne type hendelser. Heri stort og smått som å øve på hvordan man responderer på trusler, men også det å øve i og sammen med en sikkerhetsorganisasjon, og erfare hvordan den fungerer. Ergo øve på flere nivåer. Deri øve på phishing-trusler, hvordan systemene responderer på sikkerhetstrusler, det med sikkerhetsmonitorering og annen overvåkning.

> «Og så vil det alltid være utfordring når det kommer til det med varsling og varslingsrutiner. Og spesielt i en så stor organisasjon.»

Skolesjef mente at det er viktig å ta en overordnet vurdering. At alle tjenester er viktige, at eksempelvis skole er et stort volum hvor det er mange pcer, det er mye digital drift, alt fra skolekontor nivå, til administrasjon ute på skolen og til elevene. Hun hadde derfor ønsket en mer direkte link inn i kriseledelsen. I situasjonen som oppsto skulle skolekontoret informere 300 ansatte, og foresatte til 1600 elever. De fikk mange

spørsmål daglig, først og fremst fra de ansatte som sto i mange tekniske dagligdagse ting. Dermed mente hun også informasjon fra kriseledelsen som handlet om data og enhet skole skulle vært mer synlig på grunn av vansker med kommunikasjon som de opplevde og frustrasjonen rundt det. Ett av eksemplene hun trekker frem er dette med feilpålogging, og hvor mange runder man kan ha med det? Kunne det vært et par alternativer som lå beskrevet i en beredskapsplan, slik at når problemet oppsto så ville svaret være «sånn gjør vi det»? I tillegg mente hun at det også handler om hvordan man håndterer stress. Hvordan håndterer man en uforutsett situasjon der man skal prioritere?

I tillegg mener hun at man må øve for å være så godt forberedt som mulig. Og å øve på og å tenke igjennom hva man gjør hvis dette skjer. Hvordan får man informasjon ut til foresatte, hva skal man informere de ansatte om, hvordan kan man drive skole. Er man trygge på hvordan man har lagret data på servere om elevene, spesielt de dataene man har som er sensitive.

Personvernombud foreslår helt konkret oppgaver som man kunne ha gitt, hvilken informasjon kan være lekket eller er lekket, altså løse det og finne ut av det og kategorisere.

> «Det hadde vært en veldig god greie. Det er fra fordi at det er så innmari viktig og det er én ting er å oppfylle lovverket - nå starter man jo den kriminelle løpebanen så fort man egentlig begynner i en kommune sånn i ytterste konsekvens, fordi at ansvarsområdene nesten uansett hvor i næringskjeden man er så er det forpliktelser man har som er veldig lett å bryte, men alvorlighetsgraden av det er jo noe annet. Dersom viktig informasjon lekker her for en person som bor på sperret adresse for eksempel, så kan det ha en fatal konsekvens. Ja det har jeg lært mye om. Nå har jeg jobbet med mye forskjellig og jeg tenker egentlig ofte på at man skal være litt varsom der, men man ser liksom ytterste konsekvenser da når noe sånt skjer.»

Og for eksempel for å øve en type varslingsgruppe, så mener hun at hvordan den bør være sammensatt også er en viktig del av øvelsen. En kommune bør etter hennes oppfatning ikke rigge spesialister på alle disse områdene, men man må ha en plan for hvem man kontakter på samme måte som når man skal man skal evakuere, deri hvilken kompetanse bør denne gruppen bør ha. Og som hun sier «ligger det i planen, så er det jo egentlig å trykke på knappen og få de inn».

Innsatsleder IKT mener at Østre Toten, og dermed andre, burde ha risikoforståelse sånn at man skjønner at dette er en reell risiko og at det er katastrofalt hvis det skjer, eller når det skjer – for det skjer jo.

> «Du veit jo at det skjer, det skjer hele tida. De må ha risikoforståelse for at dette er noe som skjer, og hvor ille det faktisk kan bli i praksis. Og da trenger du jo kompetanse for å jobbe med risiko, du må skjønne trusselen, og hva det betyr når det skjer. Det er i alle fall kompetanse som offentlig sektor trenger. Og det tror jeg egentlig du trenger i alle kommuner. Jeg tror ikke du kan ha ei gruppe i KS eller ei gruppe i et eller annet departement eller noe, du må ha det ute der beslutningene tas. For den andre enden av dette er at vi må investere i ett eller annet, bruke penger og ressurser på noe, og da er vi tilbake til det jeg pratet på. Vi må bygge infrastruktur og teknologi, som i størst mulig grad

> lønner seg, du må bygge sikkerhetskultur, du må lære opp folk til å oppføre seg riktig i cyber-domenet. Og det vet jeg jo, ikke minst etter den her erfaringen, at selv om teknologien stopper så og så mye trusler, så er det alltid noen som kommer igjennom, da truslene utvikler seg hele tiden. Folka er alltid den siste skansen på en måte.»

I tillegg påpekte han beredskap, beredskapsforståelse og beredskapsplaner og å øve på dette.

> «For det gjør man jo ellers i beredskap. Du later som om noe skjer, og så prøver du å håndtere det. Det koster jo og tid og penger. Og da er vi tilbake til det å forstå hva det er viktig å bruke tid og penger på.»

Fylkesberedskapssjef mener at for å begynne med øvelser, så er det jo det å øve på det som kan bli potensialet, at man lager et scenario som her, men kanskje ikke absolutt alt, sette stab og trene ut ifra et kommune-perspektiv. Mot et undervisningsperspektiv mener han at man må være involvert i undervisninga, at man i tillegg til et teknisk aspekt også må se på overgangen til det operative perspektivet.

> «Hva dette har å bety for de som driver med den operative håndteringen, kommunedirektøren da, kommuneperspektivet og hva kommunedirektøren trenger å vite. Hvilke systemer er kompromittert, hvilke kan jeg bruke, kan vi bruke dem allikevel, ikke sant. Hvilke systemer er helt nede som vi ikke kan bruke, hva er konsekvensen av det, hvor lang tid tar det, hvilke deler av min bedrift er ramma, dette er jo sånne ting som kommunedirektøren vil vite om.»

Sikkerhetskonsulenten fra ATEA anbefaler at hvis man klarer å gjøre en øvelse på slike forhold så er det bra. ATEA kjører liknende simuleringer for selskaper, og etter deres erfaring, så klarer man da å finne ut hvem som er best egnet til det ulike roller, da det gjerne kommer opp litt fagkunnskap til de som deltar. Etter deres erfaring er det jo kommunikasjonsavdelingen eller fagenheter, som sammen som tar seg av det med pressen, mens det er kommunedirektøren eller tilsvarende som tar så selve politi/er ansvarlig for politianmeldelse og rapportering til statlige myndigheter. Gjerne med bistand fra IT-sjef.

> «CERT-ene har ikke noe annet enn en rådgivende funksjon slik jeg ser det, og har ikke annen mulighet enn å påvirke dem gjøre de antallet «patcher» og gjøre opp igjen oppmerksom på sårbarheter. … Det blir litt for ja, det blir mange CERT-er som rapporterer akkurat det samme. Det burde jo vært et samarbeid mellom de forskjellige CERT-ene og NSM i større grad synes jeg da, sånn at man kan få litt «intel» og noen prosedyrer rundt dette. Sånn som vi ser det nå så har jeg gjort en del modenhetsanalyser rundt omkring i forskjellige bedrifter og kommuner og det er veldig mange som ikke har en forskjell på en IT hendelse og en vanlig hendelse, slik som en flom eller strømutfall eller sånn, eller annet altså. En IT-sikkerhetshendelse, på en måte innebærer en del andre ting også; isolering, rapportering, kartlegging av hva slags data som kan være. Det er mange det er mange ting som er i tillegg i forhold til en vanlig innsats da.»

ATEA har hittil ved forberedelser til øvelser gjort en simulering på ledelsesnivå, at de har satt seg sammen i et «krisemøte». Som sikkerhetskonsulenten presiserte gir ikke nødvendigvis dette en god nok forståelse av at back-up er nede og utilgjengelig og hva dette faktisk betyr.

*Hadde du tenkt på noe før intervjuet som du tenkte det var viktig å fortelle meg for at man skal lære av hendelsen?*

Økonomisjef ønsket å formidle at de som er ansatt i kommunen er jo til for dem som bruker dem og som trenger dem.

> «Det er innbyggere i ulike settinger, noen ganger så er de jo da takknemlige, men noen ganger så er det noe krevede.»

Dermed mener økonomisjefen at det er viktig at kommune-samfunnet ikke stopper fordi at man opplever en krise, og det å ha høyde for at selv om man har en krise så må vi ikke glemme hvorfor man er til.

> «For en tid siden så hadde vi en øvelse knyttet opp mot at alle kommunikasjonssystemer var nede, og da hadde vi inn en tur som var god på sånn, som driver med radiokommunikasjon. Ja ulike typer måter å kommunisere på. Og det var lærerikt for meg i den forstand at det ikke bare finnes det noen tekniske løsninger du ikke vet om, men også da hva kan du få til hvis du er flink til å improvisere. Og jeg mener jo at det vi gjorde med å improvisere og få til at vi kunne jobbe for kommunen i en annen kommune, og vi brukte jo NAV i Vestre Toten til å være vårt system for våre NAV-brukere i denne perioden. Så hadde det noen sider i etterkant, for det er jo noe som skal avstemmes, men det var det å se etter muligheter utenfor kommunen da. Men jeg tror et læringspunkt vil jo være at det er noen grunnleggende regler i samfunnet som du ikke kan droppe selv om du er i krise. Det er noen lover som gjelder. Men se folkene dine, følg med folka dine hvordan det går, og særlig når det går jo lang tid. Og være åpen og ærlig. Så langt du kan. Jeg tror vi har tjent på det, jeg tror at våre innbyggere ville ha hatt en annen holdning til oss som organisasjon, men også til selve krisen hvis vi hadde satt lokk på den. Så jeg tror vi har tjent enormt på å ha en åpen og ærlig kommunikasjon underveis. Og ikke prøve å forklare bortforklare at vi ikke var gode nok.»

Han mener også at det er en viktig erfaring å ta med seg i det videre arbeidet at man måtte tenke strategisk fra dag 1, og det var noe av det mest krevende som de hadde vært med på.

> «Det at vi både skulle takle det at IT-folkene våre jobbet døgnet rundt, samtidig som vi da drev og planla for at de skulle slutte å jobbe hos oss. Fordi det tok 6 uker i fra dette her skjedde til vi da hadde fått tatt den strategiske beslutningen at vi ikke skulle gjenoppbygge vår egen dataavdeling. Så det var jo noen heftige timer der vi da drev og vurderte de ulike alternativene, og vi vi hadde jo ikke side opp og side ned med utredninger om dette ikke sant. «Dette er hendelsen, og vi skal bort i fra det, og vi skal forebygge dette». Om vi må da ta en beslutning, skal vi skal vi gjøre sånn, skal vi gjøre sånn, eller skal vi gjøre sånn – det finnes det noen prosedyrer når du har med folk gjøre.

> Og skal du gjøre endringer for folkene så finnes det jo noen etablerte prosedyrer for det, og så skulle vi gjennomføre det parallelt med at de jobber døgnet rundt for at vi skal komme opp igjen å gå. Det var relativt krevende, må si det. Og det var altså krevende å si at, ja i det øyeblikket vi har tatt en beslutning, så er det ingen vei tilbake. Vi jobber jo underveis med tanke på at ja nå skal vi komme opp å gå, og så og så kom det til noen punkter der vi hadde noen som fortalte oss at dette går ikke. «Vi klarer ikke å oppnå det de vil ved å gjøre det på den måten.» Det var krevende å parallelt jobbe i krise og samtidig jobbe strategisk for enhver framtid. I forlengelse av dette, når vi valgte da å legge ned vår egen IKT-drift/avdeling, så sikret vi jo de ansatte, det finnes jo mekanismer som ivaretar deg, men dette skjedde så konsentrert og når den beslutningen var tatt på en torsdag så skulle vi da få den nye samarbeidspartneren vår IKOMM til å planlegge sammen med oss og starte det på fredag. Og når vi da hadde mye oppe i løpet av kort interim drift i mars og over til normal drift i november, men vi brukte da noen få uker til å planlegge den her nye driften der de andre bruker halvannet år. En ting er at det var krevende for oss, men vi har jo pushet andre også i denne situasjonen. Så vi ville hatt en annen et annet tidsforløp hvis vi hadde møtt en type partner som ikke hadde hatt evne eller mulighet eller vilje til å sette oss øverst på prioriteringslisten.»

Kommunen tok denne beslutningen med bakgrunn av den situasjonen de sto i, men økonomisjef påpeker at han vil ikke påstå at de hadde tatt den samme beslutningen dersom de hadde hatt mer tid til å gjennomføre prosessen.

> «Vi sto i den situasjonen vi gjorde, og vi hadde et valg mellom alternativene som fantes, og det valget var nok også litt betinget av og preget av situasjonen vi sto i.  Ja for det vi visste var at vi måtte ta et valg på framtida, men samtidig så visste vi at det er kanskje ikke tidspunktet nå for å og ta det mest usikre valget, eller mest spenstige valget, eller det mest uferdige alternativet. Vi mente jo at vi tok dette på alvor, sannsynligvis vil det være like mange folk på IT hos oss som før hendelsen, men det er anna kompetanse.»

Et annet område økonomisjef ønsket å nevne var hvorvidt de har klart å kommunisere godt nok i enhver sammenheng.

> «Fordi denne utålmodigheten i organisasjonen, denne frustrasjon når ting, når vi sier at ja vi er nå er vi 70% opp å gå, da begynner jo å forventningen å komme. Om at ja nå er det vår tur, og da er det ikke bare vår tur til å komme opp å gå, nei da er det også vår tur til å bli prioritert på nye ting, nye prosjekter som vi har på gang. De vil vi gjerne realisere nå. Og vi var så godt i gang i mars, vi hadde god progresjon, og så lekket data på nettet, det mørke nettet, og da fikk det en ny dimensjon. Vi måtte snu oss rundt. Og så særlig etter sommerferien så var disse forventningene til at ja nå skal vi se sånn ut, hvor vi har vi fått klare anbefalinger, så kommunedirektøren og bestilte rapport for å få vite hva det er vi må vi gjøre for å sikre oss, og for at vi er utsatt for ikke skal skje en gang til. Det har vi fått klare anbefalinger på, og i tillegg så har vi jo vi da også laget vår vurdering av sikkerheten eller gjennomgangen hos IKOMM som gjør at vi har mange felles læringspunkter for å bli bedre i tida framover. Så kommer sikkerhetssituasjonen i Europa etter Ukraina ble okkupert /krigen

> startet, med fokus på sikkerhet, så vi jobber jo nå parallelt med å forbedre sikkerheten vår, samtidig som vi skal drive ordinær drift. Og så har vi den ressursen vi har på dette som vi har, og så må vi fremdeles bremse. Nå er vi snart midt i 2022, vi hadde innbrudd i begynnelsen januar i 2021, vi kommer til å bruke hele dette i året og kanskje også mye til neste år for å nå igjennom lista med forbedringspunkter. Som krever tid, ressurser, oppmerksomhet, og som gjør at vi må bremse denne her utviklingstakten.»

Personvernombudet ønsket å påpeke hvilken viktig funksjon for å oppfylle denne forordningen personvernombudet har.

> «Og at det er ikke en ulempe at det er en person som har i hvert fall samfunnet i bakhodet, og som er relativt autonom.»

Innsatsleder IKT ønsket å formidle at selv om han er sikker på at trengs folk ut i kommunene, det trengs folk der beslutningene tas som har en forståelse for dette her, slik det er i dag, så trenger de også hjelp i fra andre. Eksperter på å forberede for dette her, og planlegge for det, og skjønne risikoen. Han mener man trenger ekspert-bistand uansett. Han mener dermed at i offentlig sektor ville det vært naturlig at det ble lagt til rette for et eller annet sted.

> «Det burde vært noen som kan hjelpe kommunene, og de ressurspersonene som sitter ute i kommunene. Oppe i dette her som jeg ikke har sagt så mye om, så fikk vi jo en del hjelp fra KS. Han som var fagansvarlig for personsikkerhet og slikt. Det var jo hjelp det, og jeg hadde dialog med ham. Den ene er at den hjelpa vi fikk av ham var av hans egen interesse i dette her. Den egeninteressen han hadde i det, det var mange grunner til det, han hadde helt åpenbart en agenda, med å gå så hardt inn i dette her og hjelpe oss, både ift KS, men og personlig, men det er for så vidt greit nok og ikke så interessant. Det som er interessant er at han personlig hadde interesse av å hjelpe oss så mye, han hadde ingen rolle, og det var ingen systematikk. Det var han personlig som tiltrådte den rollen. Det er verdt å merke seg, og det er viktig å vite for å se på hvordan man må bygge opp dette for det offentlige. Han kjente folkene fra KPMG og sånne som har jobbet i dette andre miljøet tidligere. Jeg tror du kan telle på ganske få hender de folka som virkelig kan med disse tingene, og som har jobbet med det i praksis i Norge. Poenget, og det viktige med dette er at han hjalp oss som individ, fordi han ville og kunne. Dette var ikke satt i system, og hadde det vært noen andre i hans sted i KS, eller andre omstendigheter så hadde vi gått glipp av masse hjelp, og håndteringen av situasjonen kunne vært helt annerledes.»

I tillegg ville han nevne at det NC3 og NSM gjorde var å tappe oss for informasjon for å kunne komme videre i saken, som ikke hjalp kommunen på noe vis.

> «De dro jo ingen ting inn i å hjelpe oss, annet enn noen støttende ord – de var jo hyggelige folk. Men deres interesse var helt åpenbart kun for sitt eget arbeid og sin egen etterforskning. Og det er jo litt sånn betenkelig. Jeg tenker at hvis man skal gjøre noe for kommunal sektor så burde du hatt det SWAT-teamet som kanskje ikke blir så stort og brutalt som jeg skulle ønske at det var. Det var jo det jeg følte at de tilfeldige ressursene som de fra KPMG var tilfeldigvis

> og heldigvis akkurat de rette folka som hadde akkurat rett kompetanse og erfaring. Og det var det jo han fra KS som visste om – den gruppa med folk. Så det var vel kanskje den mest nyttige hjelpa vi fikk av ham, at «jeg vet at der og der jobber sånn og sånn», og dagen etter satt disse på møterommet på Østre Toten. Og så tok vi sammen kontroll over situasjonen. Og det var det største lettelses sukket jeg har tatt noensinne.»

For øvrig mente han at teknologi og sikkerhet, mennesker og sikkerhet og beredskapsplaner er det viktigste å ha fokus på. «Alt annet vil være å dukke for mye ned i detaljer.»

Fylkesberedskapssjef ville gjerne påpeke at man må evne å ha en situasjonsforståelse på flere nivåer. At det ikke er det samme situasjonsforståelse for teknikerne som det er for kommunedirektøren eller en hvilken som helst direktør.

> «En hvilkens om helst operativ og strategisk ledelse er mest interessert i å vite hva dette betyr for meg og min drift, så ikke veldig sånn, når det er tekniske aspekter så er vi mest interesserte i å vite hvor lang tid ting tar. Hvor lenge vi er «svarte» nå. Så det man er interessert i der, og ikke nødvendigvis de tekniske utfordringene man har da, og det er kanskje litt uheldig fordi det er jo noe tekniske løsninger som man også bør ha kontroll på. Det her med forskjell på online-backup og separat back-up er for eksempel kan jo være en strategisk beslutning, og da finner man kanskje ut at online back-up kanskje ikke er det største trikset i verden. Det at man klarer å kompromittere back-up samtidig som man kompromitterer øvrig system er jo i høyeste grad en reel fare da, som kanskje bør tas tiltak på for å unngå. Nå rammet denne cyber-hendelsen en kommune, som nå kanskje er en sånn noenlunde oversiktlig greie, det er kanskje noen som vil mene at det var vanskelig å få oversikt, men det er utrolig mye mindre komplisert enn om det er et sykehus som hadde blitt satt ut da. Som har ressurser på et helt annet nivå enn en kommune. Det fins jo aktører i staten som gjør at du er nødt til å ressurssette på en helt annen måte når ting er «svart». Derfor er vi så opptatt av at det er en beredskapsplan med tiltak for dette.»

Sikkerhetskonsulenten fra ATEA ville gjerne påpeke at det er under-kommunikasjon på omfanget av IT systemer og særlig i kommuner hvor det er såpass komplekst. Som han nevnte, er det er mange fagsystemer, det er mange divisjoner, det er mange brukere som bruker dette, men det er gjerne lite vilje til å investere i nødvendig sikkerhet.

> «Eksempelvis å sette seg inn i enkle ting sånn som Microsoft har noe som heter LAPS, et gratis system som folk kan installere på 2 timer og så får de unike passord på alle administratorer brukerne på PC-ene. Gratis, tar 2 timer å installere, men folk kjenner ikke til det ikke sant. De har ikke tid til å finne ut av de enkle tingene så er det ofte når vi kommer inn og gjør sånne analyser og modenhetsanalyser, så gir vi noen tips for å for å få dem i hvert fall opp på et visst nivå. Men det er investeringsviljen og eller evne til å se at ting kan over skikkelig galt da så som så svikter ofte. I hvert fall å ha en ordentlig back-up som ikke noen hackere kan komme til. Og så er det veldig mange som ikke har tatt en BIA da for å finne ut av hvilke systemer som er viktige, altså prioritere de systemene, der er det veldig mange som ikke har tatt de

nødvendige analysene da. Og så er det selvfølgelig rutiner ja som ligger i bunnen, opplæring og rutiner av personell rett og slett. De fleste kommuner har jo ikke SIEM løsninger heller. Man må definere noe «use cases» og få lagt inn det, og så når du da har varslingen på plass, hvem skal få de varslingene, for det skjer jo døgnet rundt ikke sant, det må jo være personell som faktisk skjønner dette og hva de blir varslet om.»

NTNU

Kunnskap for en bedre verden

VE

ISBN 978-82-326-6051-3 (printed ver.)
ISBN 978-82-326-5292-1 (electronic ver.)
ISSN 1503-8181 (printed ver.)
ISSN 2703-8084 (online ver.)





NTNU

Norwegian University of
Science and Technology