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.

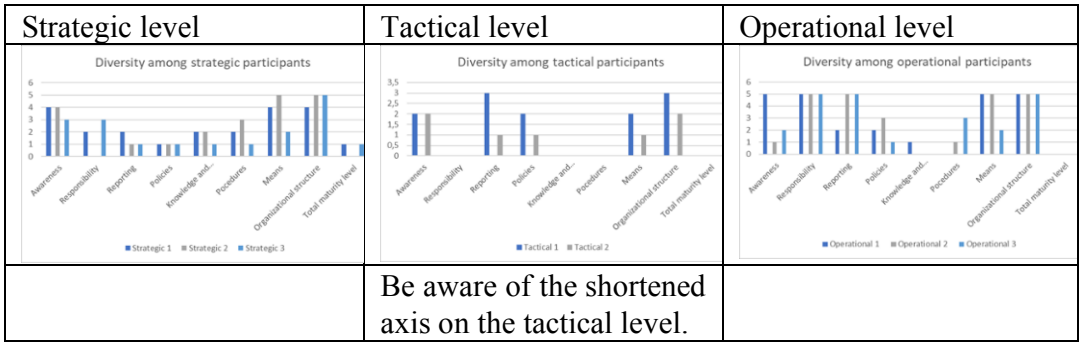

Figure 2. Maturity results on strategic, tactical and operational levels [3]

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.

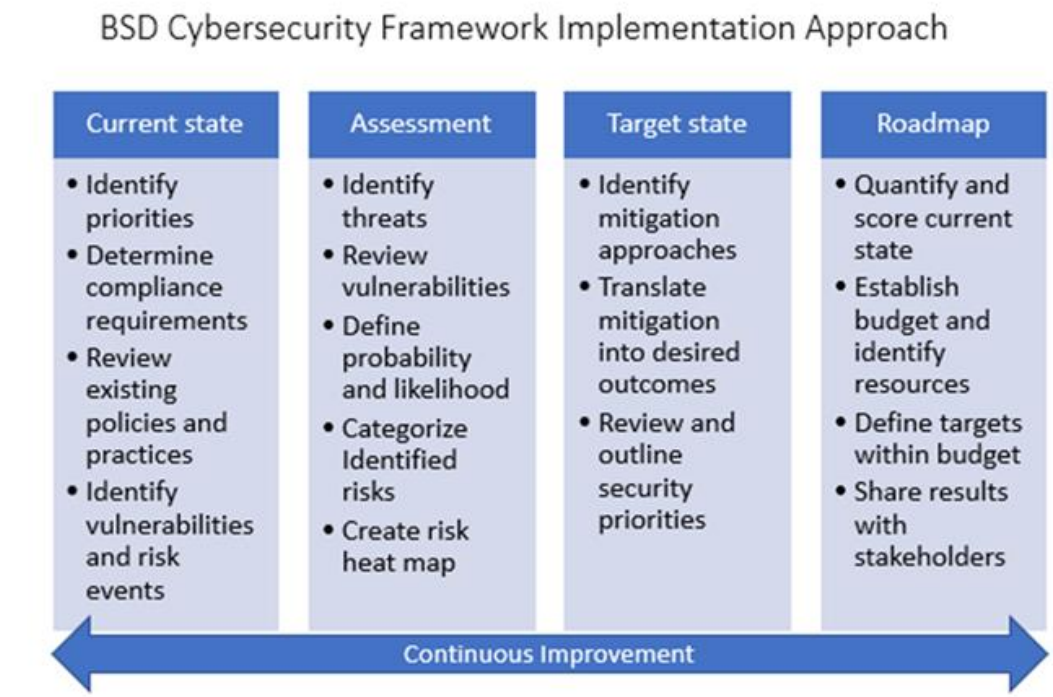

Figure 3. NIST improvement process in Chicago BSD work [14]

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:

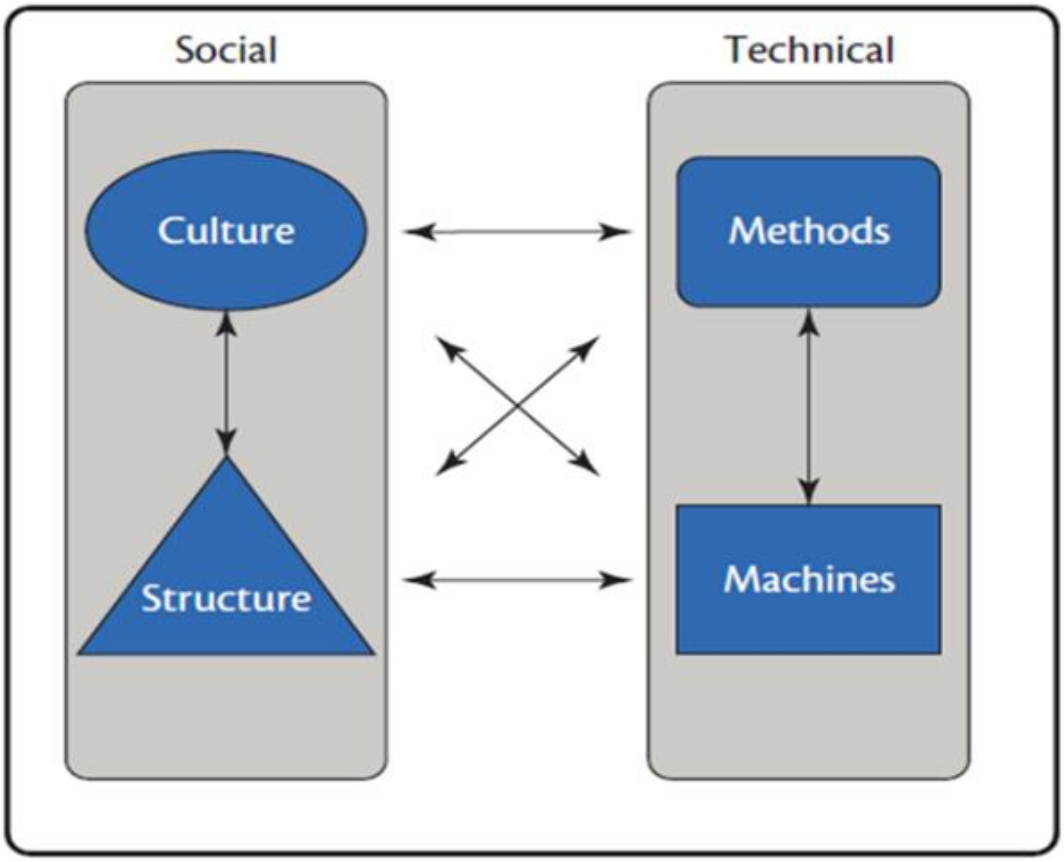

Figure 4. Socio-technical approach [15]

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.

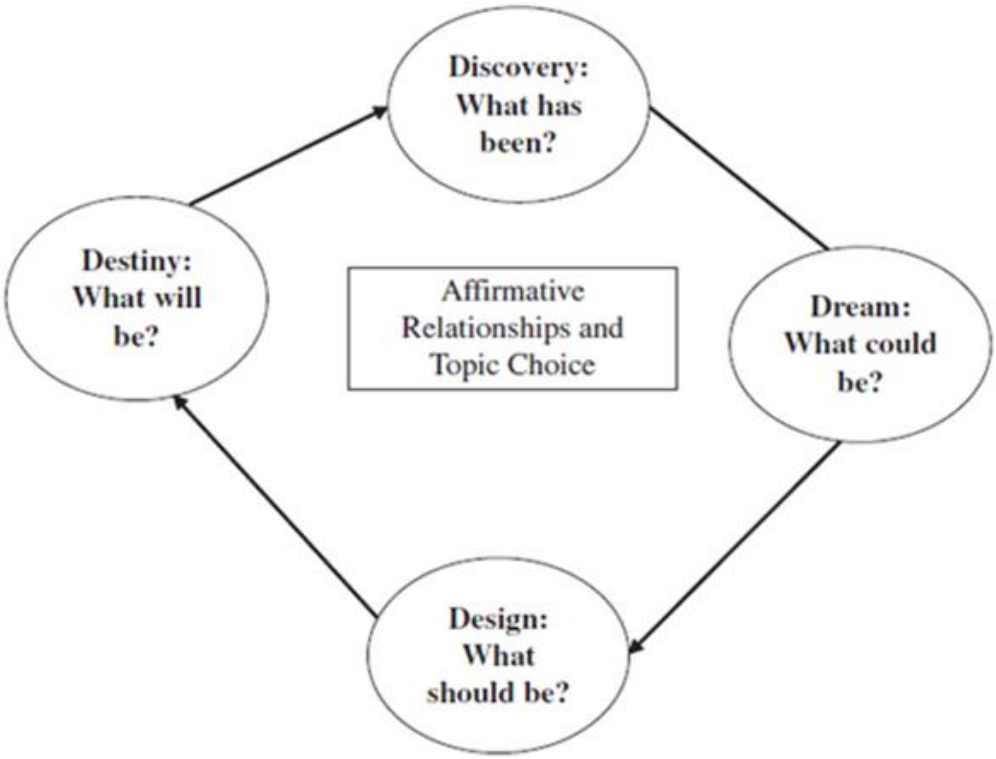

Figure 5. Appreciative inquiry approach to leader development [17].

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.

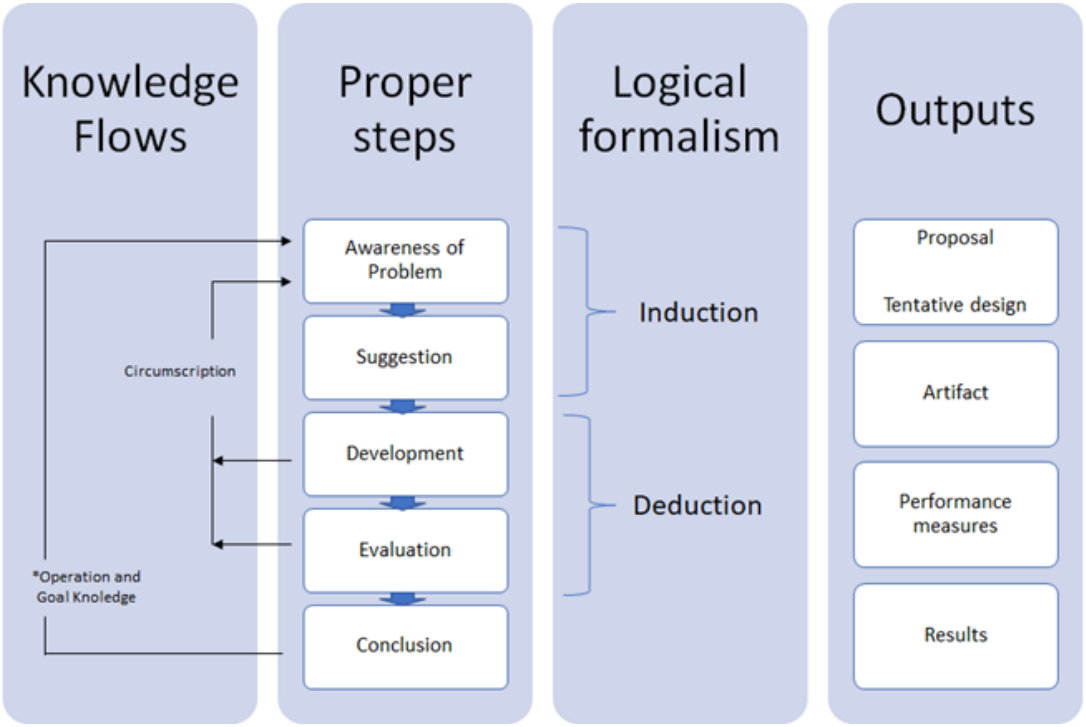

Figure 6. Design research methodology – modified

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).

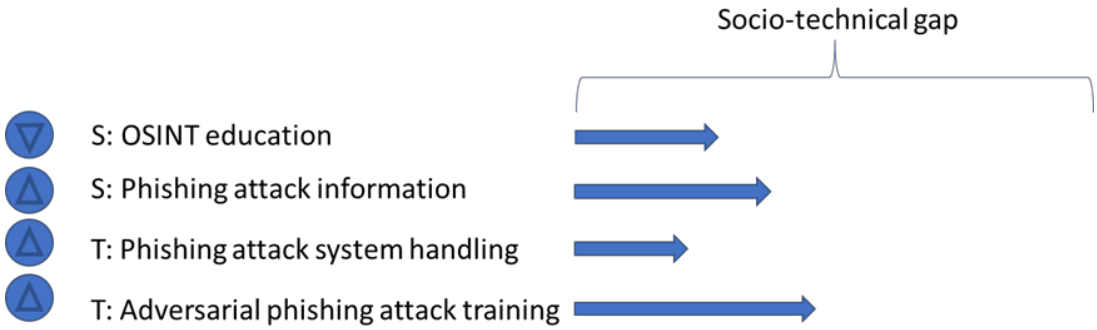

Figure 8. Granular suggestions effect on closing the socio-technical gap

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 S: Phishing attack information T: Phishing attack system handling 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.

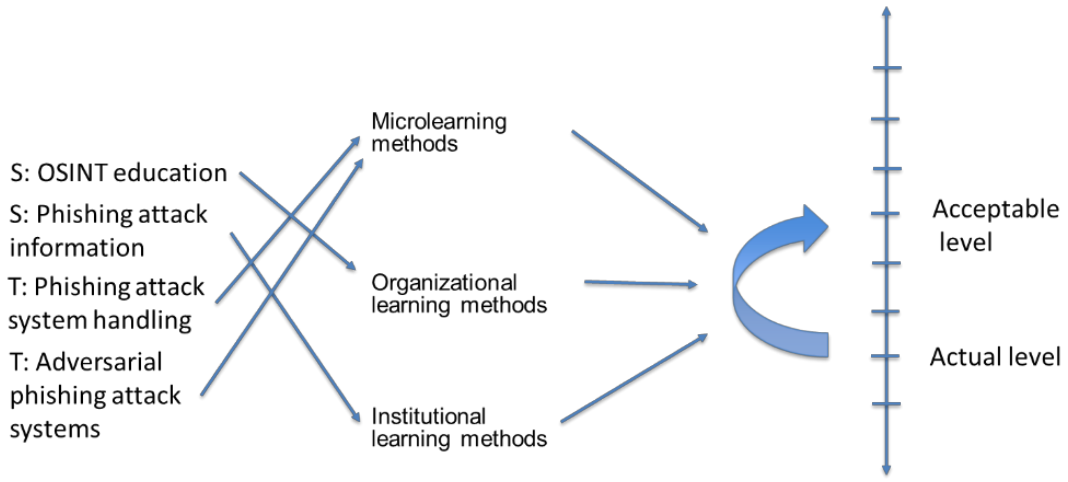

Figure 10. Implement processes to learn action points

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.