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.

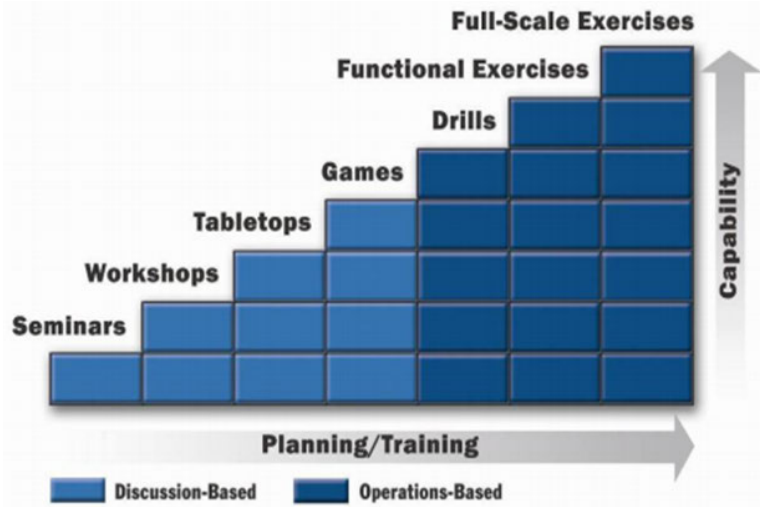


Figure 1. Exercise Types and Capacity Levels [12]

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.

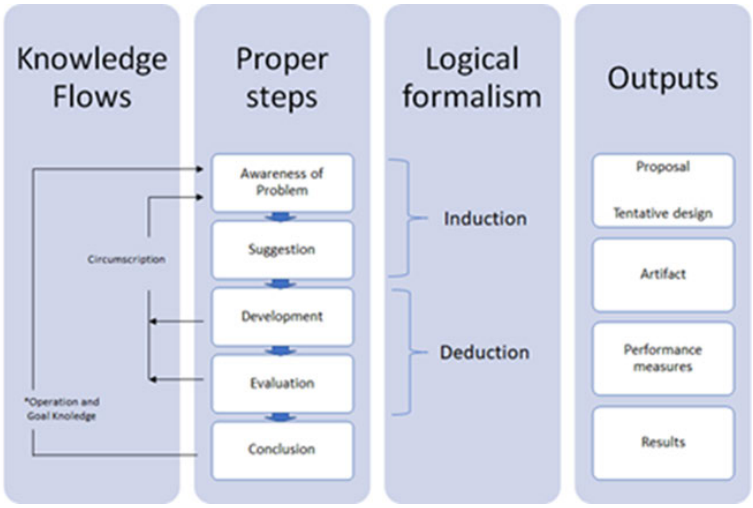


Figure 2. DSRIS – modified from abduction to induction [31]

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.

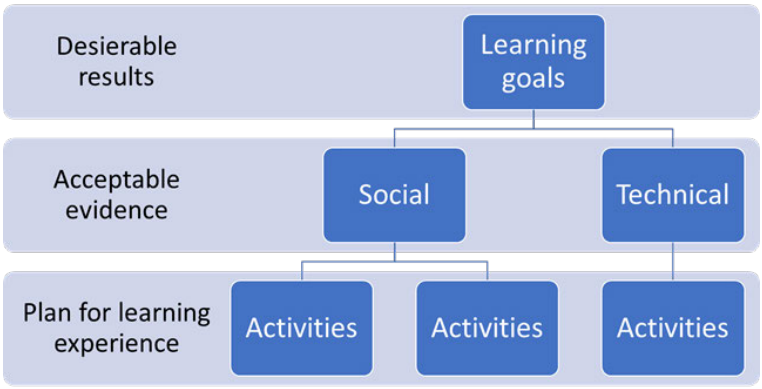


Figure 3: Backward Design, modified in a socio-technical context [32], [20]

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.

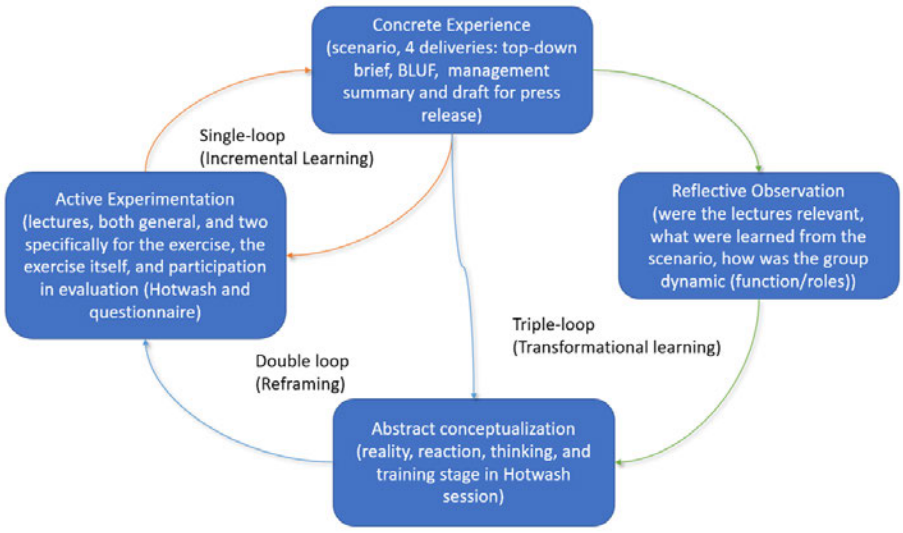


Figure 4: Pathways of and outcomes of single-, double- and triple-loop learning adapted from Medema [29]

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.

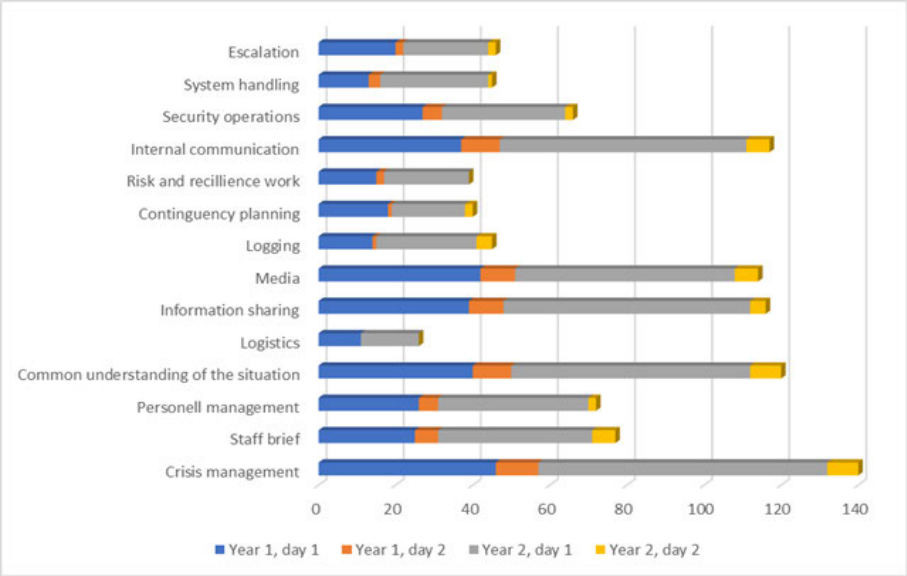


Figure 5: Factors in the scenario the student scored as achieved.

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).

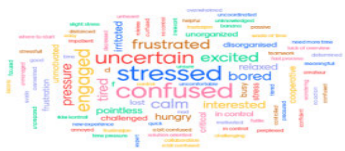
5.4 Student deliveries

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" "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" "Who is responsible for what is important"	"Important to know what type of incidents that might occur"
Year 2, day 2	"Communication is essential" "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.