An empirical study of socio-technical information security exercises as a tool to foster organizational learning and information security readiness development in Norwegian municipalities

Guro B. Olsborg[1,*], Grethe Østby[1], Mohamed Abomhara[1] and Sule Yildirim Yayilgan[1]

[1]*Norwegian University of Science and Technology, Department of Information Security and Communication Technology, Teknologivegen 22, 2815 Gjøvik, NORWAY*

Abstract

This study examines how socio-technical design elements in information security exercises can promote learning in Norwegian municipalities facing significant competence gaps in information security. Drawing on interviews with participants (n=8) from IT and crisis management teams in four Norwegian municipalities one year after participants attended a combined crisis management and information security exercise, we employ thematic analysis to examine learning outcomes through a socio-technical lens that includes culture, structure, methods, and machines. Our findings indicate that the exercise design successfully facilitated double loop learning in particular. Evidence of single-loop learning was also found throughout our socio-technical analysis framework. Evidence of triple-loop learning (organizational transformation) was more limited, but present in structural changes implemented in two of four participating organizations and reflections on inter-municipal cooperation and organizational resilience. The findings indicate that socio-technical exercise design particularly strengthened cultural awareness of information security priorities and exposed structural gaps between IT-teams and crisis management teams. This study extends Østby and Kowalski's[1][2][3] socio-technical exercise framework by providing empirical evidence of multi-level learning outcomes in municipal information security exercise contexts.

Keywords

socio-technical, exercise design, information security, organizational learning, multi-loop learning

1. Introduction

Norway's national cybersecurity strategy emphasizes the role of exercises, stating that both public and private entities should prioritize contingency exercises in relation to critical digital infrastructure[4]. With five out of ten Norwegian municipalities reporting critical competence gaps that hinder their cybersecurity development[4], the need for effective organizational learning through exercises has become increasingly urgent. The government acknowledged in Meld. St. 9 (2022–2023)[5, p. 28] that "in a challenging economic situation, it will however be difficult for the municipalities to set the necessary priorities and acquire cyber security expertise". The Digital Norway of the Future[6, p. 33] reaffirmed that "exercises and collaboration are crucial to strengthening security and emergency preparedness" in the current security policy landscape. Against this backdrop, our research examines how socio-technical design of information security exercises can facilitate the organizational learning necessary to address these challenges, potentially offering a pathway for municipalities to develop the capabilities envisioned in national strategy[4], and supporting Norway's strategic priority for municipalities to strengthen their information security preparedness.

Previous studies have shown that while participants in exercises learn from the learning objects introduced in exercise directives and scenarios[2], the new knowledge stays at the individual level and

The 11th International Workshop on Socio-Technical Perspectives in IS (STPIS'25) September 17-18 2025 Skopje, North Macedonia.

[*] Corresponding author.

guro.b.olsborg@ntnu.no (G. B. Olsborg); grethe.ostby@ntnu.no (G. Østby); mohamed.abomhara@ntnu.no (M. Abomhara); sule.yildirim@ntnu.no (S. Y. Yayilgan)

0009-0004-1228-7229 (G. B. Olsborg); 0000-0002-7541-6233 (G. Østby); 0000-0001-9151-7694 (M. Abomhara); 0000-0002-1982-6609 (S. Y. Yayilgan)

does not contribute to triple-loop learning and therefore does not appear to trigger necessary changes (transformation) in organizations[2]. This work presents a follow-up interview study performed one year after four information security exercises were conducted with Norwegian municipalities. The four municipalities attended a combined crisis management and cyber-security exercise at the Norwegian Cyber Range (NCR)/Norwegian University of Science and Technology (NTNU) in the spring of 2024, one exercise for each municipality. In this study we performed qualitative interviews and present results from these interviews that question whether exercises can bridge the gap between technical skill development and a need for organizational transformation. The study utilizes rich qualitative data from semi-structured interviews to further investigate whether and how transformative learning can potentially be reached through information security exercises. We offer insight into the relationship between exercise-based learning and organizational information security improvements.

After the introduction, we present the background for the exercises and relevant studies of information security exercises. We thereby provide our theoretical foundations for developing the analysis framework for the study. The study's methodology is presented in the Method section. Findings are then presented, structured according to our proposed socio-technical and organizational learning analysis framework. Finally, we conclude and suggest future research based on some of this study's limitations.

2. Background and theoretical framework

In this section we present the exercise design and framework, before we present theoretical foundations on socio-technical systems, and organizational learning.

2.1. Background and design of the studied socio-technical information security exercises

This study is a part of a research project conducted over a period of 2 years, initiated by previous studies on single, double and triple-loop-learning artifacts in full-scale cyber-security exercises[3]. The overall project covers 1) action research when researchers participated in the exercises, 2) immediate post-exercise evaluation-results from the participants of the exercises, 3) socio-technical questionnaires before the exercises, and one year after the exercises, and finally 4) qualitative interviews with participants one year after the exercises. This study presents the interview process and analysis of the empirical data from 4), the qualitative interviews.

The exercises were prepared for[1], and conducted, based on the assumption that the preparations and execution should give learning outcomes the organizations to initiate transformational changes from what would be referred to as triple-loop-learning artifacts[3]. The practicalities in this work were conducted as a project-collaboration between the four municipalities attending the exercises, and The Norwegian University of Science and Technology (NTNU)/The Norwegian Cyber Range (NCR), and were funded by the Innlandet county governor. The project's steering committee gave a mandate to execute the research mentioned in the early stages of the project. The research project itself is independent of the exercise project and is funded by the research institution - The Norwegian University of Science and Technology.

Full-scale exercises are the most complex operations-based type of exercises, and they involve elements of real-time resource mobilization across multiple organizations to test crisis management capabilities and validate emergency response procedures[7]. The information security exercises in this study can be referred to as full-scale exercises, since crisis management (therein information management) in the municipalities, combined with the municipalities' technical incident-management, and next-level sectorial continuity management were trained in the same exercise. As a full-scale exercise, it was a combined discussion and operations-based training, and contained aspects from all types of exercises as described in the HSEEP manual for exercises[7]. Østby's recent research[3] indicates that these types of exercises provide better learning outcomes and may actually transform the way the municipalities approach cyber-security threats and thereby prepare for crises- and incident management. An early indication of such changes appeared when the largest municipality announced cyber-attack as the second most serious risk in their public risk-assessment shortly after the exercise was conducted[8].

The implementation and operational aspects of in the municipality exercises consisted of:

1. A socio-technical maturity investigation within each municipality and interviews with potential participants to exhale desired exercise goals within each municipality.
2. Development of a cyber-range test-bed to be able to train on 4 main technical issues – 1) Surveillance – and action upon alarms, 2) Isolation, 3) search in logs, and 4) firewall-administration. The test-bed were developed to be as similar to a security-zone divided municipality system-architecture as possible, though only 4 applications were used compared to a normal environment with approximately 250 applications and systems.
3. Preparation of an exercise directive and a time-lined dynamic scenario with step-by-step socio-technical learning objectives and backward design socio-technical learning activities in lectures before the exercises, and in instructions and timeouts/lectures within the exercises.
4. Walk-through with the instructors and EXCON-teams beforehand the exercises (instructors and EXCON-team played 'the world' and adapted actions and decisions done in the municipalities into the played scenario) for them to be in line with intended learning activities especially prepared for the municipality at hand.
5. Execution of the exercises.
6. Group evaluation of the exercise.

All of the operational aspects explained above were prepared with socio-technical approaches. Our study builds on an established theoretical foundation that combines socio-technical systems theory with organizational learning frameworks, specifically developed for information security contexts[3]. We draw on the theoretical work developed through collaborative research with Østby and colleagues[3][9][1]. This pre-established theoretical background will be explained in the following.

2.2. Socio-technical systems theory and information security preparedness

In this study we have structured our research and findings into a socio-technical approach as developed by Kowalski[10]. Kowalski's socio-technical framework, see Figure 1, was a modification of Leavitt's[11] organizational change model, which originally comprised four interconnected elements: people, task, structure, and technology. Building on the Tavistock Institute tradition established by Mumford[12], who emphasized that "technical and human factors should, whenever possible, be given equal weight in the design process"[12, p. 323], Kowalski adapted these principles for information security contexts. His framework[10, p 9] is based on two basic components; a social subsystem and a technical subsystem - see also[12]. Within these two subsystems, Kowalski re-conceptualizes Leavitt's four elements into four components[10, p 9]: *Culture* which is connected to values[10, p. 9] and behaviors of the teams and individuals[13, p. 54] which again are part of the everyday practices in an organization[13, p. 50]; *Structure* that refers to the organization's formal and informal setup and central authority[13, p. 54]; *Methods* which are the processes and techniques used in relation to technology[13, p. 54]; and finally*Machines* which is the technology component of the framework[13, p. 54][10][14].

Figure 1 provides an overview of the two subsystems and the four components that are interconnected, as illustrated through arrows which point back and forth between all elements. The interconnectedness in Kowalski's[10] framework illustrates that technical IT security measures alone are insufficient. If we are to apply information security exercises as a measure to create learning conditions that can facilitate necessary organizational learning and provide opportunities for organizational transformation needed to improve information security preparedness, technical security measures will need to be integrated with organizational culture, structure, and methods in the exercise design and implementation[10][3][13].

2.3. Organizational learning theory: Single- double- and triple-loop learning

Triple-loop learning theory is a concept from organizational learning literature. As presented by Medema, Wals, and Adamowski[15] and adapted to the context of information security exercises by

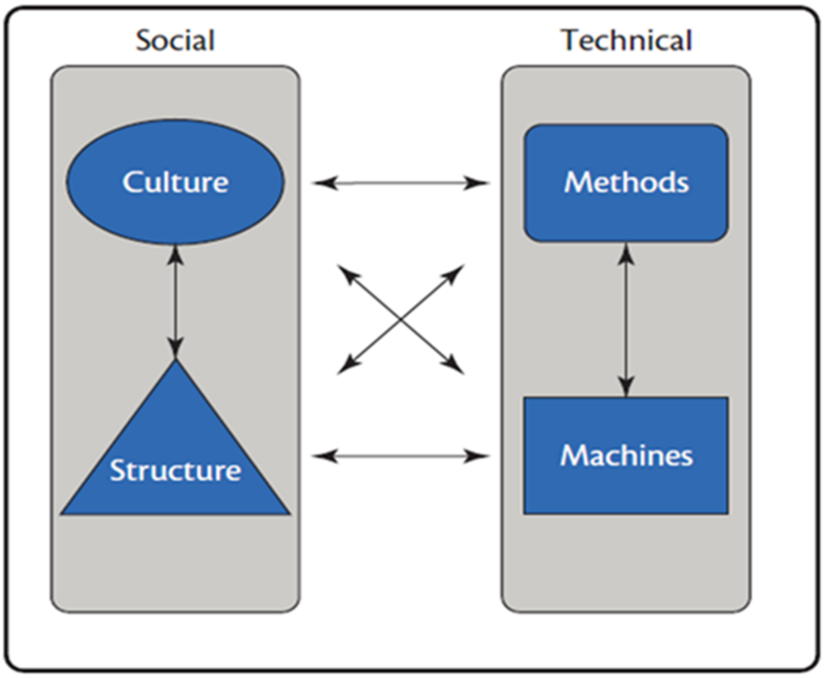


Figure 1: Socio-technical framework[1]

Østby and Kowalski[1][2], the concept entails three levels of organizational learning. Medema et al.[15, pp. 26–28] present that single-loop learning enables the learner to address immediate operational adjustments within existing frameworks (”Are we doing things right?”); double-loop learning enables the learner to question underlying assumptions and revise accordingly (”Are we doing the right things?”); and triple-loop learning enables a more fundamental reflexivity and meta-learning through reflection on learning processes (”How do we decide what is right?”).

Single-loop learning occurs when organizations refine techniques and methods to achieve better results within the boundaries of current organizational paradigms[15, p. 26]. Double-loop learning moves beyond technical refinements to examine whether organizational objectives, assumptions, norms, and policies should be revised[15, p. 27]. Triple-loop learning has been conceptualized not only in terms of cognitive transformation (meta-learning), but also as learning that can enable structural and governance transformation[16]. Medema et al.[15] emphasize that triple-loop learning may lead to ”institutional changes, such as changes in structures, policies, programs, rules and decision-making procedures”[15, p. 27].

2.4. Integrated theoretical framework - learning levels and socio-tecnical components

Østby and Kowalski[1] developed an integrated socio-technical and learning theory framework to facilitate organizational learning through information security exercises. Their work demonstrated how discussion exercises can function as deeper learning artifacts, moving beyond simple skill development to enable triple-loop learning in information security management contexts.

Figure 2 visualizes the pathways and outcomes of single-, double-, and triple-loop learning adapted to the context of information security exercises from a figure by Medema et al.[15, p.28]. Figure 2 presents how each learning level builds upon the previous while addressing increasingly fundamental organizational questions[3], and lists specific learning artifacts (listed within parentheses), which have been built into the design of the information security exercises[2]. The progression from active experimentation in incremental single-loop learning, to reframing through abstract conceptualization, and then to transformational learning through reflective observation at the triple-loop level demonstrates how discussion exercises can facilitate learning at all three levels within one and the same exercise[1].

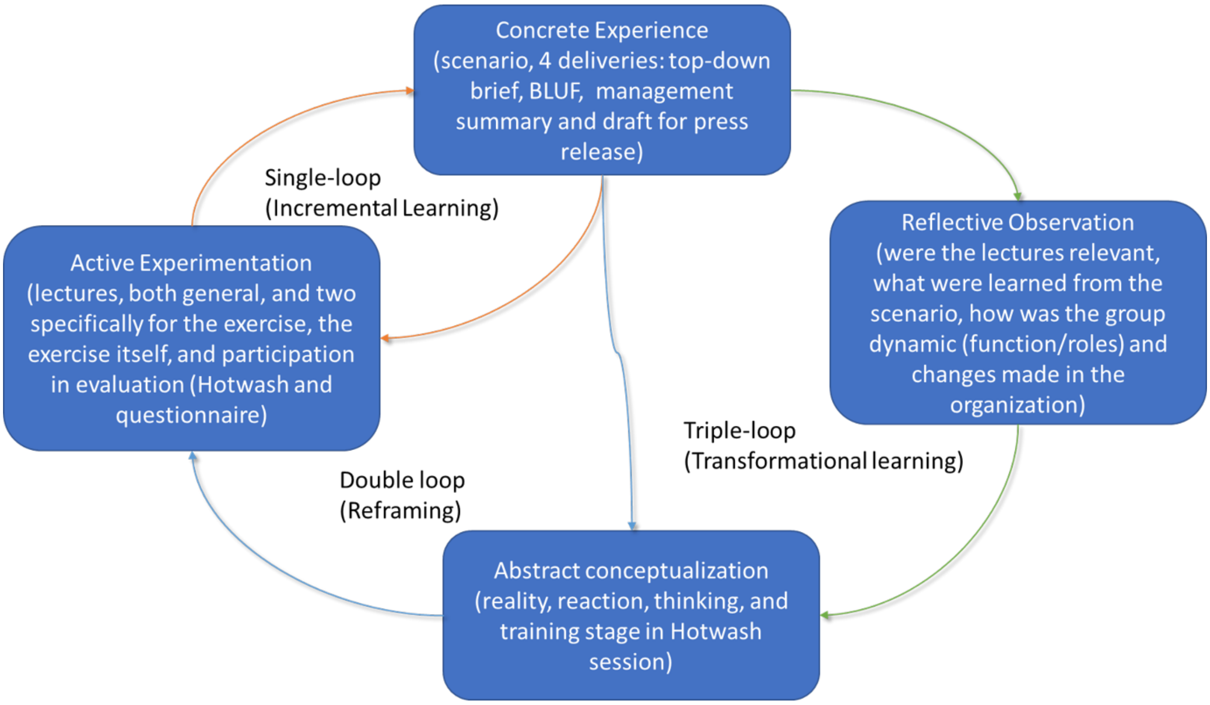

Concrete Experience (scenario, 4 deliveries: top-down brief, BLUF, management summary and draft for press release)
Reflective Observation (were the lectures relevant, what were learned from the scenario, how was the group dynamic (function/roles) and changes made in the organization)
Abstract conceptualization (reality, reaction, thinking, and training stage in Hotwash session)
Active Experimentation (lectures, both general, and two specifically for the exercise, the exercise itself, and participation in evaluation (Hotwash and questionnaire)
Single-loop (Incremental Learning)
Double loop (Reframing)
Triple-loop (Transformational learning)

Figure 2: Single, double and triple-loop-learning artifacts, modified[3]

Østby and Kowalski suggest that by conceptualizing discussion exercises within this framework, organizations can meet socio-technical incident response challenges through multi-loop learning[3].

3. Method

This study builds on socio-technical analysis as an approach through which we examine how exercise design elements facilitate learning across the three learning levels and the four socio-technical components[3]. An analysis of a data set from 8 semi-structured interviews was performed to examine some of the participants' own reported experiences and reflections on organizational outcomes.

3.1. Research question and aim

Behind this study is the larger question of whether and how transformative learning could be achieved through socio-technical design of information security exercises. More specifically, this study asks the research question *RQ1: To what extent do socio-technical information security exercises facilitate organizational transformation through multi-level learning in municipal organizations?*

By examining the specific experiences reported by participants in socio-technical information security exercises as described by Østby and colleagues[3], we aim to offer practical insight into the relationship between municipal organizations' learning processes, and organizational information security preparedness improvements.

3.2. Qualitative interview study design and participant selection

Eight semi-structured interviews were conducted in March and April 2025, approximately one year after the exercises took place in 2024. This timing allowed participants to reflect on more long-term organizational impacts while still maintaining memories of the exercise process and the exercise experience itself.

Interview candidates from the four participating municipalities were contacted, making an effort to recruit one interview subject from the IT team, and one interview subject from the crisis management team. Adjustments were made as we prioritized interviewing two representatives from each municipality in cases where we were unable to recruit participants from both of the teams. The interview subjects had all participated in the exercises, either as part of an EXCON-team, or as a member of the municipal IT- or crisis management team. See table 1 for an overview of interview subjects according to which municipality they worked in and which exercise team they participated in.

Table 1
Overview of Interview Participants

Interview information	Municipality
Interview #1, IT team manager	Municipality 3
Interview #2, IT team manager, member of EXCON-teams	Municipality 2
Interview #3, member of EXCON-teams	Municipality 1
Interview #4, member of crisis management	Municipality 3
Interview #5, member of crisis management	Municipality 1
Interview #6, member of crisis management	Municipality 2
Interview #7, member of crisis management	Municipality 4
Interview #8, member of crisis management	Municipality 4

3.3. Interview process, data privacy and ethical considerations

All interviews were conducted and transcribed in Norwegian by the first author of this study. The semi-structured interview guide contained open-ended reflection questions, provided in translation (from Norwegian to English) in Appendix A. Interview questions were relatively open-ended and focused on participants' experiences during the exercise, learning outcomes, and whether or not they had experienced any subsequent organizational changes. Interviews lasted 30-60 minutes and were conducted via video conferencing to accommodate participants' schedules and geographical distribution (in-person interviews were offered as an equally available option, but all participants requested video conference interviews).

Translation of the interview transcription was conducted in conjunction with our reported findings, where it is relevant to demonstrate such quotes and excerpts. As a privacy measure, full transcripts will not be published, and the study provides excerpts from the interviews rather than full transcripts. We will not reference the quotes and excerpts to the participant overview, as this could also potentially identify participants. Privacy protection measures were also taken during the interview and transcription process. These measures were important in order to reassure the subjects that they could report their experiences honestly and openly to the research project.

Measures were taken to analyze data in a way that separated the role of the principal investigator of the research project and the contributing author who also participated in the exercise project itself; Interviews were performed and transcribed solely by the first author, and the data set was kept separately. The two final authors have seen and discussed the data set and coding with the first author.

3.4. Qualitative interview data analysis method: Abductive thematic analysis

As Thompson[17, p. 1411] notes, research in the social sciences can be broadly divided among deductive (theory-testing), inductive (exploratory and interpretive), and abductive (theory-refining or iterative between theory and data) research designs. According to Thompson[17], the widely used method thematic analysis[18] aligns with an inductive research paradigm. This is why Thompson[17, p. 1411] argues that when existing theory or frameworks play a guiding role in coding and thematic development, researchers should acknowledge that they are utilizing an abductive methodological research approach.

We selected Thompson's abductive approach[17] for our study as the goal was to analyze how existing socio-technical and organizational learning theories could explain participants' experiences, and then inform and guide the design of future exercises. The analysis of the interview data proceeded according to Thompson's[17, pp. 1412–1418] framework for abductive qualitative analysis. We hereby present a short overview of how we carried out these steps in practice:

1. Interviews were conducted in Norwegian and auto-transcribed. The principal investigator then listened to and corrected all transcriptions. The participant's own syntax and wording was kept, but punctuation was added to improve readability. The primary investigator then conducted an active read-through with annotations in NVivo to identify initial patterns and areas of (theoretical) interest.
2. Coding was performed with multiple rounds of coding to refine and consolidate related codes.
3. A simple codebook was developed and revised in the step when codes were refined and consolidated.
4. Codes were then grouped into themes. These themes were developed to capture both explicit participant statements and latent meanings that required theoretical interpretation. We constructed the themes from the codes, and not from the theoretical framework, to ensure that we included unexpected findings from our data analysis, which could potentially prove important for future work to further develop the current theoretical frameworks (in accordance with[17, p. 1411]).
5. In step 5, we re-examined the themes through the lens of our theoretical foundations of socio-technical and organizational learning theories. We then created a 3x4 analytical matrix which allowed systematic examination of how exercise design elements facilitated different levels of learning (single-, double-, or triple-loop learning) across all socio-technical components (culture, structure, methods, and machines).
6. Step 6, comparison of data sets, was not applicable for our present interview study which consists of only one data set.
7. Step 7, data display, was omitted from this study for brevity.
8. Write-up of the findings is presented in section 4 of this study.

4. Findings

Our interview study demonstrates that the socio-technical system elements in the exercises facilitated multi-loop learning. We argue that the exercises' comprehensive approach could ensure that the organization not only addresses immediate issues but can also drive deeper, long-term improvements related to information security readiness. Examples of both successful and unsuccessful outcomes are demonstrated and discussed in relation to the exercise design when we report our findings in the following.

Since the study's analysis framework is quite extensive, we present all the themes in a table format in Table 2. The table shows an overview of all themes in accordance with the learning-loop level and the socio-technical component in question for each theme, and could be used for reference when one reads through the findings.

In the following findings, we present each one of these themes, relating them to the learning-loop level and the socio-technical component. To keep the presentation of findings as concise and brief as possible, we include cross-references to concrete citations of participants' statements for each of the themes rather than to include the participant statements in the text itself.

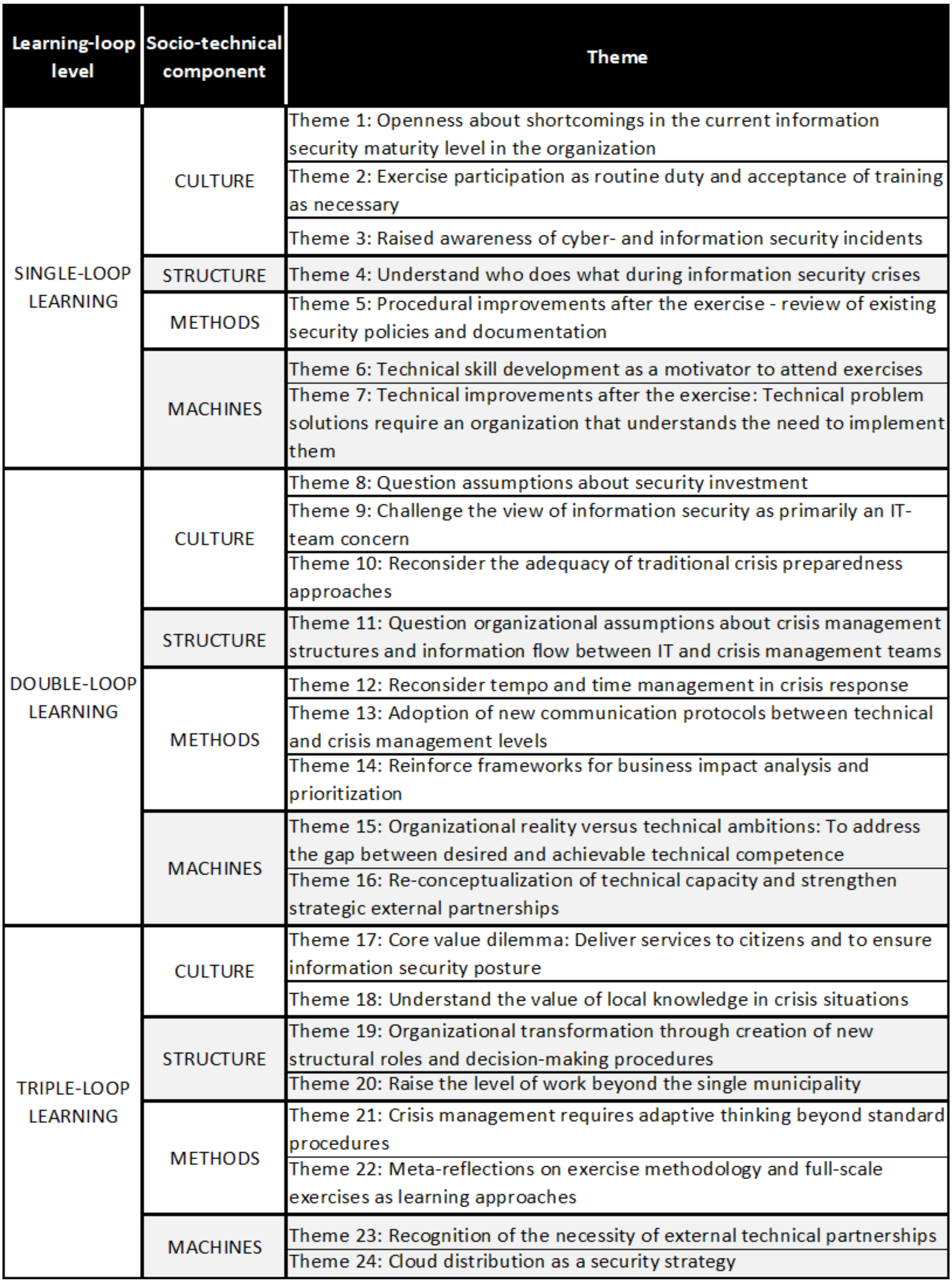
4.1. Single-loop learning

In summary, we found that single-loop learning was facilitated by technical skill development, procedural refinements - particularly if the organization had prepared for the exercise - and scenario elements that provided opportunities for operational problem-solving.

4.1.1. Single-loop learning: Socio-technical component Culture

We found three main single-loop learning themes related to the socio-technical culture component, each of which we will explain below.

Table 2
Overview of all themes in findings presented in a nested table firstly by learning loop level and secondly by socio-technical components.



Learning-loop level	Socio-technical component	Theme
SINGLE-LOOP LEARNING	CULTURE	Theme 1: Openness about shortcomings in the current information security maturity level in the organization
		Theme 2: Exercise participation as routine duty and acceptance of training as necessary
		Theme 3: Raised awareness of cyber- and information security incidents
	STRUCTURE	Theme 4: Understand who does what during information security crises
	METHODS	Theme 5: Procedural improvements after the exercise - review of existing security policies and documentation
	MACHINES	Theme 6: Technical skill development as a motivator to attend exercises
		Theme 7: Technical improvements after the exercise: Technical problem solutions require an organization that understands the need to implement them
DOUBLE-LOOP LEARNING	CULTURE	Theme 8: Question assumptions about security investment
		Theme 9: Challenge the view of information security as primarily an IT-team concern
		Theme 10: Reconsider the adequacy of traditional crisis preparedness approaches
	STRUCTURE	Theme 11: Question organizational assumptions about crisis management structures and information flow between IT and crisis management teams
	METHODS	Theme 12: Reconsider tempo and time management in crisis response
		Theme 13: Adoption of new communication protocols between technical and crisis management levels
		Theme 14: Reinforce frameworks for business impact analysis and prioritization
	MACHINES	Theme 15: Organizational reality versus technical ambitions: To address the gap between desired and achievable technical competence
		Theme 16: Re-conceptualization of technical capacity and strengthen strategic external partnerships
TRIPLE-LOOP LEARNING	CULTURE	Theme 17: Core value dilemma: Deliver services to citizens and to ensure information security posture
		Theme 18: Understand the value of local knowledge in crisis situations
	STRUCTURE	Theme 19: Organizational transformation through creation of new structural roles and decision-making procedures
		Theme 20: Raise the level of work beyond the single municipality
	METHODS	Theme 21: Crisis management requires adaptive thinking beyond standard procedures
		Theme 22: Meta-reflections on exercise methodology and full-scale exercises as learning approaches
	MACHINES	Theme 23: Recognition of the necessity of external technical partnerships
		Theme 24: Cloud distribution as a security strategy

Theme 1: Openness about shortcomings in the current information security maturity level in the organization Several participants indicated an attitude towards to learn as they directly or indirectly expressed that they believed it is important to be honest and open about the information security maturity level in the organization. One interview subject explicitly described this as a prerequisite for

learning (see excerpt A1 B.1). Two participants expressed similar attitudes when their organization's preparations for the exercise were discussed (see excerpts A2 B.1, and A3 B.1). That same strategy was not representative for all municipalities, but an undertone of openness about shortcomings was present. One participant conveyed that they used the exercise as leverage to further their work while they still downplayed their security preparedness level (see excerpt A4 B.1). We interpret this finding as not necessarily a consequence of the exercise, but rather a sign of an existing culture of honesty and openness that contributed to participation in the exercise with an attitude of openness to change.

Theme 2: Exercise participation as routine duty and acceptance of training as necessary Most participants indicated that their organizations generally had an attitude towards information security and participating in the exercise as obligatory and necessary duty. One participant articulated this through expectations that everyone should attend (see excerpt A6 B.1). However, our analysis showed this awareness was reported to remain surface-level for some, with security still perceived as burdensome by one of the interview subject's colleagues (see excerpt A5 B.1).

Theme 3: Raised awareness of cyber- and information security incidents The culture of awareness and participation seemed to encourage incremental behavioral changes. Interview subjects indicated these changes as positive, but also somewhat limited in their potential for deeper changes (see excerpts A7 B.1, and A8 B.1). Another interview subject also expressed doubts that one exercise could make deeper changes (see excerpt A9 B.1). A third participant had a slightly more optimistic view, and saw the exercise as part of an incremental process (see excerpt A10 B.1).

4.1.2. Single-loop learning: Socio-technical component Structure

At the structure level, we saw that the preparations before the exercises, the lessons immediately before the exercise, and to some extent the exercise itself provided participants with opportunities to expand their knowledge of organizational roles and responsibilities in crisis management. Our analysis identified one key theme that indicated single-loop learning in the socio-technical structure component.

Theme 4: Understand who does what during information security crises Our analysis showed that IT teams typically operate outside normal crisis management structures (see excerpt B1 B.2). The observation that IT teams were not usually part of crisis management could also be seen from descriptions of their advisory role (see excerpt B2 B.2). One participant reported that colleagues had achieved what we interpret as single-loop learning about structure in an information security crisis, but they had not necessarily proceeded to double-loop and/or triple-loop learning (see excerpt B3 B.2).

4.1.3. Single-loop learning: Socio-technical component Methods

Participants reported that the exercise helped solidify existing procedures and methods. We found one theme that indicated such incremental changes took place during and after the exercises.

Theme 5: Procedural improvements after the exercise - review of existing security policies and documentation. We find examples of incremental method changes described by participants (see excerpts C1 B.3, and C2 B.3). Another participant indicated awareness of needed plan revisions that remained work in progress one year after the exercise (see excerpt C3 B.3). Learning on this level can seem limited if we only consider single-loop aspects, but we also found that single-loop learning can point towards elements of double- and triple-loop learning themes. In one case, improvement on incident response plans sparked regional cooperation to make further improvements (see excerpt C4 B.3).

4.1.4. Single loop learning: Socio-technical component Machines

The exercises provided a test bed environment that allowed personnel to use specific crisis management tools relevant in crisis situations. The municipalities who participated requested these concrete tools to both learn system usage and test organizational adaptation. This was part of the exercise goals and user-focused approach presented in the background section.

Another technical aspect was the Norwegian Cyber Range's contribution of a live virtual technical platform for IT teams. This platform developed significantly as the exercises progressed, and lead different municipalities to report very different experiences. The exercise IT platform included generic servers, fictitious information systems, and network setup with monitoring tools for live events.

Participants reported some technical improvements after the exercise. It was also pointed out that there was a need for single-loop learning in other parts of municipal organizations, not just technical skills development in the IT-teams. We found three themes that belong to this learning level and socio-technical component.

Theme 6: Technical skill development as a motivator to attend exercises All participants suggested that the exercise provided opportunities to learn a new crisis management system tool recently acquired by the Norwegian municipal sector (see excerpt D1 B.4). A participant reflected on motivation to test the tool (see excerpt D2 B.4). One municipality experienced system unavailability during their exercise, reported by the participant in a way which demonstrated the importance of the tool training as a motivation (see excerpt D3 B.4). Similar disappointment appeared regarding the live technical platform (see excerpt D4 B.4). The technical platform provided mixed results. One participants expressed value in hands-on experience (see excerpt D6 B.4), while another found the unfamiliar platform less successful for IT staff learning (see excerpt D7 B.4). One participant reflected on tool focus potentially interfering with deeper scenario learning (see excerpt D5 B.4).

Theme 7: Technical improvements after the exercise: Technical problem solutions require an organization that understands the need to implement them Post-exercise improvements demonstrated increased concrete understanding (see excerpt D8 B.4), but these suggestions were mostly given as short and often generalized remarks (see excerpt D9 B.4). Our interpretation of this finding was that the dialog-based oral qualitative interview method may be less appropriate to capture detailed technical single-loop learning instances.

4.2. Double-loop learning

Our findings indicate that the information security exercise design was successful to facilitate double-loop learning, and found evidence of double-loop learning to a larger degree than single-loop learning. This might also potentially be attributed to our observation that the qualitative interview methodology does not facilitate a very thorough and detailed report of many small instances of incremental single-loop learning very well.

4.2.1. Double-loop learning: Socio-technical component Culture

Our thematic analysis of participants' reflections revealed questioning of fundamental cultural assumptions about information security priorities and organizational responsibilities after the exercise. While some questioning processes appear to have been ongoing within the organizations, the exercise seemed to have provided a shared experiential context that crystallized and accelerated ongoing cultural negotiations. We found three main themes which indicated this in our analysis.

Theme 8: Question assumptions about security investment Several participants described ongoing organizational tensions around security investments that the exercise helped bring into focus. These negotiations appear to have occurred both before and after the exercise, but participants suggested that the shared experience provided new leverage for discussions. One IT manager described persistent challenges with resource allocation (see excerpt E1 B.5). The same participant emphasized that political decision-makers continued to face difficult value-based tradeoffs (see excerpt E2 B.5).

Participants attributed varying degrees of change to the exercise's impact. One participant explicitly connected the exercise to a shift in organizational priorities while also pointing to multiple contributing factors (see excerpt E3 B.5). This suggested that while economic allocation challenges continued to be an issue, the exercise contributed to an environment where some of the arguments for security investment found more receptive audiences.

Theme 9: Challenge the view of information security as primarily an IT-team concern Participants identified existing organizational dynamics where information security was treated as a technical specialty isolated from broader organizational concerns. The exercise provided practical experience that reinforced ongoing efforts to broaden security responsibility across organizations. One participant articulated this, and emphasized that everyone contributes to the organizational information security vulnerability (see excerpt E4 B.5). The exercise appeared to have provided concrete experiences that highlighted limitations of narrow approaches. One participant described pre-existing dynamics of persons outside of the IT-team seeing IT as difficult to understand (see excerpt E5 B.5). IT managers described persistent organizational challenges even after increased awareness (see excerpts E6 B.5,and E7 B.5).

Theme 10: Reconsider the adequacy of traditional crisis preparedness approaches Participants reflected on contrasts between their exercise experience and traditional paper-based exercises. These reflections suggest ongoing questioning of existing preparedness approaches that the exercise likely helped clarify rather than initiate. One participant compared approaches (see excerpt E8 B.5). The interactive and dynamic experience provided a reference point to evaluate existing approaches (see excerpt E9 B.5).

4.2.2. Double-loop learning: Socio-technical component Structure

Our analysis showed that the exercise revealed assumptions behind organizational interfaces and decision-making hierarchies in information security crisis handling that participants began to question. The exercises exposed problematic aspects of organizational design and collaboration between and within teams. Rather than to simply identify communication breakdowns, participants recognized that existing structural arrangements were inadequate to manage information security crises effectively. We found one overarching theme in our analysis that pointed towards this.

Theme 11: Question organizational assumptions about crisis management structures and information flow between IT and crisis management teams Participants observed that conventional crisis management structures, which they reported worked effectively for traditional municipal incidents, proved inadequate for information security crises. This recognition led them to question basic assumptions about how crisis management should be organized in these types of crises. One participant detailed how their normal crisis management approach completely broke down during the exercise (see excerpt F1 B.6). The same participant reflected on why this structural breakdown occurred and touched on fundamental questions about crisis management decision-making (see excerpt F2 B.6). Another participant confirmed similar structural challenges (see excerpt F3 B.6). The recognition that information security crises require different organizational capabilities led to structural innovations for two of the four municipalities. One participant described implementation of new information flow systems (see excerpt F4 B.6). A central insight was that information security incidents requires a different structure of cooperation that handles the interface between technical expertise and crisis management decision-making (see excerpt F5 B.6).

4.2.3. Double-loop learning: Socio-technical component Methods

Our analysis showed that the exercise revealed assumptions behind crisis management methodologies and procedures that participants then began to question. Participation exposed problematic aspects of how information security crises are approached compared to traditional municipal incidents. Several municipalities presented that they had implemented new methods and procedures as direct results of their exercise experiences. Rather than simply improving within existing procedures, participants recognized that their approach to IT incidents was inadequate and required new frameworks for crisis handling. We found three double-loop learning related themes relevant to this socio-technical component in our analysis.

Theme 12: Reconsider tempo and time management in crisis response Participants observed that conventional crisis management methodologies, which rely on structured meeting cycles and deliberate decision-making processes, proved difficult to apply because of information security crisis pace. This recognition led to questions about how crisis management should be temporally organized. One participant detailed how their normal methodological approach completely broke down during the exercise (see excerpt G1 B.7). Another participant reflected on why traditional methodological time frames were inadequate as mental models for information security crises (see excerpt G2 B.7). A different participant expressed similar reflections on timeline uniqueness (see excerpt G3 B.7).

This temporal challenge led participants to reflect upon their meeting schedules and decision-making speed. The uniqueness of tempo is not only related to fast start-up phases as several participants emphasized how information security crises differ fundamentally from traditional crises in stretching out over time after the initial phases of crises (see excerpt G4 B.7). The same participant also explicitly recognized the need for longer-term resilience planning (see excerpt G5 B.7).

Theme 13: Adoption of new communication protocols between technical and crisis management levels Participants recognized that existing communication methods were inadequate to bridge the technical-management gap in information security incidents. This led them to question what constitutes effective crisis communication methods. One participant described the communication challenge between IT-team members that understands the technology and the crisis management members that usually do not possess any technical understanding of IT systems (see excerpt G6 B.7). The exercise demonstrated both necessity and difficulty of this communication challenge, with stress affecting communication quality (see excerpt G7 B.7). Several participants reflected that fixing these problems and adopting better procedures for handling communication between IT teams and crisis management is crucial as not doing so can lead to loss of capacity in technical crisis handling (see excerpt G8 B.7). The main practical solution to the communication issues reported during the exercise was adopting a top-down situational brief template provided the EXCON-team (see excerpt G9 B.7).

Theme 14: Reinforce frameworks for business impact analysis and prioritization Some participants recognized that existing methods to determine priorities in crisis situations were inadequate for IT incidents. One participant articulated this methodological gap (see excerpt G10 B.7). The exercise revealed that without systematic business impact analysis methodologies that engaged with the entire organization, the IT team and crisis managers could not effectively prioritize responses. One participant described how they reinforced their prioritization framework after the exercise (see excerpt G11 B.7). Another participant realized that while the formal terminology for business impact analysis did not stick, the experience that prioritization is crucial to have in place before eventual crises was still a lesson learned (see excerpt G12 B.7). This can also be seen as a comment on communication, illustrating the participant's practical approach where substantial work on crisis preparedness occurred even without formal terminology use.

4.2.4. Double-loop learning: Socio-technical component Machines

Double-loop learning through the socio-technical lens of machines revealed a shift in how participating municipalities understand their relationship with technology and technical capacity in crises. Participants expressed questions about underlying assumptions having to do with technical preparedness, resource allocation, and organizational capabilities in terms of technical information security preparedness. The exercise prompted participants to re-examine whether their current technical infrastructure and staffing models were adequate to handle cyber security incidents. These findings were part of two themes.

Theme 15: Organizational reality versus technical ambitions: To address the gap between desired and achievable technical competence Exercises highlighted existing organizational realities that influence municipalities' strategic decisions about technical capacity. Participants reflected on challenges to maintain specialized cyber security competence in-house (see excerpt H1 B.8). These structural limitations shaped how municipalities approached technical security goals (see excerpt H2 B.8). The realization of these constraints in technical competency and/or capacity led all the municipalities to develop strategic models that acknowledged organizational limitations while still pursuing security objectives through alternative means. The means varied across the municipalities, but all remarked on increased attention towards external partnerships and collaborative arrangements.

Theme 16: Re-conceptualization of technical capacity and strengthen strategic external partnerships For three municipalities, the exercises seemed to provide leverage to revise how the municipalities should handle information security incidents which lead to strategic shifts to implement external partnership agreements (see excerpt H3 B.8). This realization led to concrete strategic changes, with municipalities establishing formal partnerships that went beyond ad-hoc arrangements (see excerpt H4 B.8). One participant elaborated on this shift in technical information security strategy (see excerpt H5 B.8). Traditional models of municipal self-reliance in technical matters were questioned, which led to revised and new frameworks for crisis management that incorporated external expertise as a strategic component rather than an emergency fallback. Participants mostly did not attribute direct, causal connections between these changes and the exercise, but all reported exercises in general, and to some degree this particular exercise, as important pieces of the overall picture that led them to make these needed strategic shifts.

4.3. Triple-loop learning

We found that attendance at the exercises created conditions to question fundamental assumptions and attitudes within the municipality, especially within the socio-technical components of structure and methods. For the components culture and machines, we view our findings as moving towards triple-loop learning rather than the more clear cases of triple-loop learning.

4.3.1. Toward triple-loop learning: Socio-technical component Culture

In our analysis, we identified two cultural themes in participants' reflections that show that to attend the exercise facilitated to re-consider fundamental organizational values and identity. We found two themes that we can see as moving towards such triple-loop learning.

Theme 17: Core value dilemma: To deliver services to citizens and to ensure information security posture When we analyzed the interview data, we observed that the participants engaged with tensions between core objectives to 1)deliver services to citizens and 2)to build long-term information security resilience. This represents a value conflict that goes beyond operational concerns to awareness of what municipalities exist to do. Participants articulated immediate human consequences when systems fail (see excerpt I1 B.9). This perspective could imply that participants constructed their organizational identity around serving citizens, particularly vulnerable populations, which makes it difficult to invest resources in preventive security measures that might not have any immediate or visible benefits. Tensions can become pronounced given resource constraints (see excerpt I2 B.9).

Theme 18: To understand the value of local knowledge in crisis situations One participant constructed local expertise and creative problem-solving capacity as essential organizational resources in crises. This suggests potential questioning of hierarchical knowledge structures and formal authority, and moving toward to value distributed expertise and tacit knowledge throughout organizations (see excerpts I3 B.9,and I4 B.9). Such a perspectives could indicate potential shifts from formal role-based authority to competency-based leadership during crises, suggesting deeper questions about organizational structure and decision-making processes. This theme was however not prevalent in other interviews.

4.3.2. Triple-loop learning: Socio-technical component Structure

Our analysis revealed that two of four municipalities went beyond questioning assumptions to actually implement fundamental structural transformations within their information security crisis organization structures. According to our theoretical framework (see presentation of [16] [15] in section 2.3 in this paper), when organizations create new governance structures, implement new decision-making procedures, and formalize new organizational roles, this constitutes triple-loop learning. Some participants also questioned whether current governance models were sufficient to meet cross-sector information security needs. These reflections were present before exercises, as cooperation on cross-municipal levels was a direct predecessor to exercises being initiated. We identified two themes that we see as triple-loop learning instances in this sense.

Theme 19: Organizational transformation through creation of new structural roles and decision-making procedures Two municipalities implemented concrete structural innovations that represented organizational transformation. These changes went beyond improving communication to create entirely new organizational arrangements and formalized roles. One participant described their municipality's structural solution (see excerpt J1 B.10). The same participant elaborated on new information flow systems (see excerpt J2 B.10). One participant from the other municipality that implemented structural changes confirmed the necessity of such intermediary roles (see excerpt J3 B.10). These structural changes represented organizational transformation in that they created new formal roles, changed decision-making procedures, and established new governance structures for crisis management. While two municipalities achieved this level of structural transformation, the other two remained at the double-loop level.

Theme 20: To raise the level of work beyond the single municipality Our analysis identified that participants questioned whether single-municipality scope was sufficient to meet today's information security challenges. This questioning touches on municipal autonomy and self-sufficiency that have historically defined Norwegian local government (see excerpts J4 B.10, and J5 B.10). Participants do not report this as a result of exercises, but rather as a piece of the larger picture that led to innovative exercises being planned and implemented.

4.3.3. Toward triple-loop learning: Socio-technical component Methods

Our socio-technical analysis uncovered two themes from participants' understanding of crisis management approaches that could suggest triple-loop learning to somewhat different degrees.

Theme 21: Crisis management requires adaptive thinking beyond standard procedure Conceptualizing crisis management to require adaptive thinking beyond standard procedures may be seen as moving towards triple-loop learning. It is not that plans and documents are not important, but crisis situations are often found to resist standardization and predictability (see excerpt K1 B.11). This understanding implies potential philosophical shifts to embrace uncertainty and value adaptive capacity over rigid planning.

Theme 22: Meta-reflections on exercise methodology and full-scale exercises as learning approaches During interviews, participants reflected on how crisis management training should be designed and delivered. This represented meta-learning about exercises as learning approaches, where participants reflected not just on what they learned, but on how they learned and how such learning should be structured, and as such this constitutes triple loop learning as defined in our theoretical framework (see section 2.3 of this paper). Most participants discussed problems with traditional lecture-based preparation methods (see excerpt K2 B.11). As an alternative, several participants recognized the need for differentiated learning approaches, especially considering municipal capacity challenges (see excerpt K3 B.11). One participant highlighted the need to design training content for audiences with differing technical expertise levels (see excerpt K4 B.11). Another participant was less critical of the lecture content and format, but suggested such pre-requisite knowledge should come earlier in preparation (see excerpt K5 B.11).

The importance of immersion and physical separation from daily work emerged as another insight of reflexive learning-on-learning (see excerpts K6 B.11, and K7 B.11). Another participant confirmed the effectiveness of the immersive approach (see excerpt K8 B.11). Some indicated that exercise scenarios needed to create appropriate stress levels to be effective (see excerpt K9 B.11). Participants also reflected on the importance of proper preparation and clarity about exercise objectives (see excerpt K10 B.11).

4.3.4. Toward triple-loop learning: Socio-technical component Machines

Some participants reflected on whether their technological philosophy aligned with the kind of organization they are or need to become. Our analysis identified two main themes in how participants understood technology's role in organizational identity and strategy, which we interpret as moving the organizations toward triple-loop learning.

Theme 23: Recognition of the necessity of external technical partnerships We observed that participants articulated fundamental limitations to maintain internal technical capacity, which led to strategic acceptance of external dependencies. This recognition challenged assumptions about municipal self-sufficiency in the technical domain (see excerpts L1 B.12, and L2 B.12).

Theme 24: Cloud distribution as a security strategy Our analysis did not supply ample evidence of this, however one participant discussed cloud strategy as a technical approach towards reaching information security resilience that is needed for the municipality (see excerpt B.12).

5. Conclusion

This study demonstrates that well-designed socio-technical exercises offer a promising approach to address municipal information security challenges. The socio-technical exercise design was particularly successful in facilitation of double-loop learning across all municipalities that participated in an exercise. Evidence was found across all four socio-technical components culture, structure, methods, and machines, when participants questioned fundamental assumptions about security investment, organizational responsibilities, and crisis management approaches. This represents the study's strongest finding regarding the exercises' capacity to promote deeper organizational learning.

On the triple-loop learning level, our analysis revealed that two of the four municipalities achieved triple-loop learning in the structural dimension, implementing fundamental organizational transformations including new formal roles, changed decision-making procedures, and/or new governance structures for crisis management in information security crises. These findings address our research question about organizational transformation and challenges previous research[3] which has suggested that triple-loop learning is rare in organizational contexts, demonstrating that socio-technical exercises can, under certain conditions, facilitate transformational organizational learning. While the exercises successfully facilitated multi-level learning, the uneven achievement of triple-loop learning (2 of 4 municipalities achieved structural transformation) could suggest that organizational transformation through exercises depends on specific conditions or factors that warrant further investigation. Cultural and technical triple-loop learning was characterized as "moving towards" rather than fully achieve transformation.

Evidence of single-loop learning was found across all socio-technical components, but we see the need to revise the research design to potentially capture more detailed evidence of single-loop learning. Relevant to single-loop learning, articipants signaled a need to adapt the exercise concept further to align with municipal organizational needs, particularly regarding technical skills development and procedural improvements.

The study contributes to socio-technical research in information security as it demonstrates that exercise design can systematically address both technical competence development, and organizational transformation needs. The integration of Mumford's socio-technical design principles[12] with Medema's triple-loop learning framework[15] proved effective to analyze complex organizational learning outcomes in municipal information security contexts. We found that the socio-technical design of the exercises facilitated organizational learning across the analyzed socio-technical components. Our findings extend Østby and Kowalski's framework[1] by providing empirical evidence of learning progression across socio-technical components in the context of municipal organizations.

Our study has shown that well-designed exercises can contribute to build the municipal information security capabilities envisioned in Norwegian national strategy[4]. The exercises were particularly effective to help participants question assumptions and make structural changes to how IT-teams and crisis management teams work together. With Norwegian municipalities facing significant information security competence gaps, this integrated approach to exercise-based learning offers a practical pathway to build the capabilities needed to meet current and future information security readiness challenges.

5.1. Limitations and future research

This study is based on qualitative interviews with eight participants, and is not expected to be representative for all participants in the exercises. The limited sample size constrains the generalizability of findings.

The qualitative interview methodology did not facilitate very detailed reports of instances of single-loop learning, and this may have resulted in under-representation of technical skill development and procedural improvements that occurred through the exercises. Future studies could incorporate a broader mix of methods to provide further validation of single-loop learning findings. A combination of qualitative interviews with quantitative measures of organizational change, document analysis of policy modifications, and observational studies of actual crisis response could provide more comprehensive evidence of learning outcomes.

The uneven achievement of triple-loop learning across municipalities represents both a limitation of current exercise design and an important opportunity for future research to understand and address the conditions necessary for consistent organizational transformation through socio-technical information security exercises.

The study is limited to Norwegian municipalities with specific cultural, legal, and organizational contexts that may not transfer to other national or organizational settings. Norwegian municipality structures, crisis management frameworks, and information security governance may differ significantly from those in other countries. Comparative studies across different organizational types and cultural contexts could further improve socio-technical exercise design principles.

While participants reported organizational changes following the exercises, establishing direct causal relationships between exercise participation and specific organizational transformations remains challenging. Multiple factors influence municipal information security development, and our study does not claim to definitively isolate any of the exercises' specific contribution to observed changes. Research into how exercise-based learning integrates with other organizational development approaches and factors (training programs, policy development, technology implementation) could inform comprehensive capacity-building strategies. Research that extends beyond one-year follow-up could capture longer-term organizational transformation processes and assess the persistence of learning outcomes over time.

Cost-benefit analyses could examine resource investment versus organizational learning outcomes, and this could inform municipal decision-making about exercise participation and help optimize resource allocation for information security capacity and preparedness development.

Declaration on Generative AI

During the preparation of this work, the authors used Microsoft Copilot, Claude, and to a lesser degree Writeful and ChatGPT, in order to: Brainstorm ideas for, and the outline of, the paper. Copilot and Claude was also used to provide and compare different examples of phrasing, varied word use (thesaurus), correct spelling and grammar, and provide feedback on text. Claude was used to format and edit text in LaTeX, and to assist translation from Norwegian to English. After using these tools/services, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

References

[1] G. Østby, S. J. Kowalski, Preparing for Cyber Crisis Management Exercises, in: D. D. Schmorrow, C. M. Fidopiastis (Eds.), Augmented Cognition. Human Cognition and Behavior, Springer International Publishing, Cham, 2020, pp. 279–290.

[2] G. Østby, S. J. Kowalski, ORGANIZATIONAL LEARNING WITH CRISES, in: International Academy of Technology, Education and Development (IATED), IATED Academy, 2022, pp. 5215–5224. URL: https://hdl.handle.net/11250/3042637.

[3] G. Østby, Digital transformation of public security - developing tripleloop- learning artifacts to meet emerged information security incident response resilience and readiness challenges in public emergency organizations, Doctoral thesis, NTNU, 2023. URL: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3062985.

[4] Norwegian Ministeries, National Cyber Security Strategy for Norway, Technical Report, Norwegian Ministeries, 2019. URL: https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf.

[5] Norwegian Ministry of Justice and Public Security, Meld. St. 9 (2022–2023) Report to the Storting (white paper) National control and cyber resilience to safeguard national security. As open as possible, as secure as necessary, Technical Report, Norwegian Ministry of Justice and Public Security, 2023.

[6] Norwegian Ministry of Digitalisation and Public Governance, The Digital Norway of the Future – National Digitalisation Strategy 2024–2030, Technical Report D-2006 E, Norwegian Ministry of Digitalisation and Public Governance, 2024.

[7] U.S. Department of Homeland Security, Homeland Security Exercise and Evaluation Program (HSEEP), Technical Report, U.S. Department of Homeland Security, 2020. URL: https://www.fema.gov/sites/default/files/2020-04/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf.

[8] Gjøvik kommune, Helhetlig risiko- og sårbarhetsanalyse for Gjøvik kommune 2024, Technical Report, Gjøvik kommune, 2024. URL: https://www.gjovik.kommune.no/_f/p2/i7faae3a4-794f-4569-8f52-199bbffb416c/2024-2028-helhetlig-risiko-og-sarbarhetsanalyse-for-gjovik-kommune.pdf.

[9] G. Østby, S. J. Kowalski, Hendelseshåndtering ved cyber-angrepet mot Østre Toten kommune Hva kan vi lære fra håndteringen?, 2022. URL: https://www.ototen.no/_f/p1/idbd37a14-f91f-41e5-9fa2-14977f2a7977/v-10-ostre-toten.pdf.

[10] S. Kowalski, IT Insecurity: A Multi-disciplinary Inquiry, PhD Thesis, Stockholm University, 1994.

[11] H. J. Leavitt, Applied Organizational Change in Industry: Structural, Technological and Humanistic Approaches, in: Handbook of Organizations (RLE: Organizations), Routledge, 1965.

[12] E. Mumford, The story of socio-technical design: reflections on its successes, failures and potential, Information Systems Journal 16 (2006) 317–342. URL: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1365-2575.2006.00221.x. doi:10.1111/j.1365-2575.2006.00221.x.

[13] T. R. McEvoy, S. J. Kowalski, The Norwegian Cyber Range, Department of Information Security and Communication Technology, NTNU i Gjøvik, postboks 191, NO-2802 Gjøvik, Norway, Deriving Cyber Security Risks from Human and Organizational Factors – A Socio-technical Approach, Complex Systems Informatics and Modeling Quarterly (2019) 47–64. URL: https://csimq-journals.rtu.lv/csimq/article/view/csimq.2019-18.03. doi:10.7250/csimq.2019-18.03.

[14] G. Østby, S. J. Kowalski, A case study of a municipality phishing attack measures-towards a socio-technical incident management framework, 2021. URL: https://hdl.handle.net/11250/3026972.

[15] W. Medema, A. Wals, J. Adamowski, Multi-Loop Social Learning for Sustainable Land and Water Governance: Towards a Research Agenda on the Potential of Virtual Learning Platforms, NJAS:

Wageningen Journal of Life Sciences 69 (2014) 23–38. URL: https://www.tandfonline.com/doi/full/10.1016/j.njas.2014.03.003. doi:10.1016/j.njas.2014.03.003.

[16] A. Georges L. Romme, A. van Witteloostuijn, Circular organizing and triple loop learning, Journal of Organizational Change Management 12 (1999) 439–454. URL: https://doi.org/10.1108/09534819910289110. doi:10.1108/09534819910289110.

[17] J. Thompson, A Guide to Abductive Thematic Analysis, The Qualitative Report (2022). URL: https://nsuworks.nova.edu/tqr/vol27/iss5/17/. doi:10.46743/2160-3715/2022.5340.

[18] V. Braun, V. Clarke, Using thematic analysis in psychology, Qualitative Research in Psychology 3 (2006) 77–101. URL: http://www.tandfonline.com/doi/abs/10.1191/1478088706qp063oa. doi:10.1191/1478088706qp063oa.

A. Interview guide

1. Is there anything you remember particularly well now, that has stuck with you from the exercise?
2. Was there anything that you and/or your colleagues learned a lot from? (before/during/after)
3. Was there anything you/your colleagues remember as negative in connection with the exercise? (before/during/after)
4. Do you feel that the exercise was an important measure for the municipality to implement?
5. Did you experience increased support/engagement from the municipality's management after the exercise?
6. In what ways do you think the exercise may have contributed? For how long? Etc.
7. Do you believe that the exercise had a lasting effect on your and your colleagues' understanding and handling of information security in the municipality?
8. In what ways?
9. Why/why not?
10. Do you feel that the exercise changed attitudes toward information security?
11. In what way? Do you have examples? For instance: Is information security valued to a greater extent? Has there been greater understanding of/knowledge about information security?
12. Have you and possibly your group changed anything in the way you handle information security (preventive and incidents) after the 2024 exercise?
13. If yes: Can you give examples? (Keywords: Actions)
14. If no: What do you think is the reason that you haven't changed anything? Not relevant/not possible/etc.
15. Do you think that the exercise may have contributed to prioritizing information security financially and/or in terms of capacity (human resources) to a greater extent than before?
16. Conclusion: Is there anything you would like to add or elaborate on/clarify regarding what we have discussed?

B. Interview excerpts

This appendix contains interview excerpts referenced in the Findings section. All excerpts have been translated from Norwegian to English by the authors.

B.1. Single-Loop Learning: Culture

Excerpt A1: *"Yes, I think that sharing the situation is important. That's where we are, and if we are to improve, we must dare to be honest, actually."*

Excerpt A2: *"We should not boast that we were very good beforehand. We conducted the exercise without doing any major preparations. We were actually quite aware, those of us who were involved, that that's where we were. There was no reason to prettify it."*

Excerpt A3: *”We had no major preparations for the exercise. Because the goal was to find out: Where are we? The only thing we had, we had read through what [consultant] had written before. And we were aware that we had inadequate documentation. We were aware that we didn’t have good enough plans.”*

Excerpt A4: *”There was a significant effort beforehand to try to establish a plan framework that wasn’t there. We can start right there. And in that area, it was probably elevated quite a few notches in advance. So in that sense it was good that the exercise was announced, because then we actually managed to put at least a small plan framework in place.”*

Excerpt A5: *”It’s not so effective, because... I had an old colleague who has been retired for many years. He said: ’Security is just hassle and hindrance, you know.’ Because it often created extra work. Either because a solution had to be set up, or because it wasn’t straightforward for the user. It was perhaps an extra obstacle, an extra password, a PIN code. (...) And then you think such small things are difficult if they don’t provide anything concrete.”*

Excerpt A6: *”And top management must be absolutely clear and explicit that this is something we should prioritize. And I think that in our exercise, even though this was announced well in advance, there were some who didn’t participate in the entire exercise. It’s clear that this diminishes the whole exercise for us as an organization. Then you don’t get as much benefit from it, I think.”*

Excerpt A7: *”So in that sense, there has been focus on it. It’s easier to talk about security in the systems after that exercise. Yes, but if we do that, like: -Security first! -Yes, yes, you’re right about that! You know, things like that. Such positive things are absolutely good, but...how quickly they understand their systems... I mean, it’s quite a scenario.”*

Excerpt A8: *”So overall, I think they started with a little experience that this was... Wow, it was extensive, right? So that if something happens, then it’s critical. And especially in IT, because it goes so fast. (...) So the engagement was perhaps that... -Oh, what a job we in ICT got. -Oh, my God, what you have to keep track of! And things like that. But how long it lasted, that’s another matter. Because it’s back to everyday work afterwards.”*

Excerpt A9: *”It has had an awareness-raising effect. It definitely has. They understand a bit more when we start to talk about loss of telecommunications, loss of power. It makes it a bit more recognizable, because we have sort of deep-dived a bit into the problem of absence of our electronic systems. But whether they have any greater and deeper understanding of information security, or the problem we ran with [the exercise?], I’m a bit uncertain about.”*

Excerpt A10: *”And to have such types of exercises as exercise tools contributes to a very significant awareness regarding which levels the different people should work at, where they should be, and what competence is required of each individual to fulfill their role. Both within the crisis management team optimally, but also between the different teams that we use when there’s an ICT incident. It was enormously useful for us, and it has been one of the most important work tools to move forward with that work.”*

B.2. Single-Loop Learning: Structure

Excerpt B1: *”IT here has never had... I mean. We’re not part of the emergency preparedness group. So: We get called in when there’s a crisis, but we don’t document anywhere. Or: We document, but we don’t document in the old emergency preparedness system.”*

Excerpt B2: *”The main answer generally is that the crisis management team is not all-knowing, and the crisis management team is completely dependent on good advice from those who actually know. That is, those who have their boots on the ground, and those who have expertise in the area.”*

Excerpt B3: *”For example, with the security organization, which was formally decided, but which we have had many discussions about afterwards regarding responsibilities and tasks and how we should do it, internal control and such things. And we haven’t reached our goal there, but we have had some discussions. And often it’s discussions that are needed to perhaps move it forward. But for me, sitting close to it, I naturally want there to be even more focus to get greater progress. Because when there are lots of discussions and we don’t always end the discussion with some clear, definite answers, we feel a bit like: Yes, then a year passes quickly.”*

B.3. Single-Loop Learning: Methods

Excerpt C1: *"I think some have reflected a bit on exactly... I mean, have made some small moves in their organization. Thought about how you should communicate, established alternative communication forms, and such things."*

Excerpt C2: *"And we have also gotten even better plan frameworks with action cards and so on. We have... We have been better trained in using [Crisis Management System] and all that IT support around crises."*

Excerpt C3: *"Execution has not turned out to be the biggest challenge, it seems, for what we have had of both exercises and situations. But what concerns emergency preparedness plans, plan frameworks, so that it becomes somewhat seamless in the organization. That one must work even more with that. That still stands."*

Excerpt C4: *"This has also resulted in a completely new ICT incident response plan, with privacy sections, which was actually implemented this year, which has accomplished quite a lot in terms of organization, information flow, governance. We are still working to refine it, and we actually have a larger project to perhaps do it on a regional level. We have applied for funding to carry it out, but we are the guinea pig ourselves now."*

B.4. Single-Loop Learning: Machines

Excerpt D1: *"The crisis management exercise specifically came right after the introduction of [crisis management tool] as a new system, at least for us to use. And really put the finger on many of the challenges that we both have had and actually have with the use of the system."*

Excerpt D2: *"I think such a system is valuable in order to have everything in one place. That you have everything you need there. But then there's also a need to learn and understand the system."*

Excerpt D3: *"And (...) we used [crisis management tool] for the first time. It crashed. It didn't work for the first two and a half hours. We had a backup solution available, in the form of Excel sheets and PowerPoints to get things logged and run meetings, but that wasn't optimal."*

Excerpt D4: *"Yes, organizationally, I think the exercise seemed well-facilitated, well-planned, well-organized. But technically, there were things that didn't work."*

Excerpt D5: *"It was a completely new tool for everyone to use right then and there. And I do think that, for the sake of the incident, it was a bit unfortunate, because the ICT incident, as an ICT incident, was extremely relevant — both then, and is still now. And I felt that the system, both now and back then, takes away the focus from the actual incident. And that's important when we train. At least I try to remind myself of that—that we need to practice just as much on the incident itself, not just the system tool. And that's a bit difficult, because when you don't have the system tool, the foundation of the system tool, in place, it's hard to lift your gaze to the incident."*

Excerpt D6: *"OK, I take down the internet line, I do this, right, and then it's: Oh! Then there's a lot of other work I have to think about. I have to inform management, I have to... you know, things like that. It doesn't become that: 'Yes, [Name], do you have anything from IT?' In tabletop exercises, where they sit and write with pen and paper, right, it doesn't become...here you get involved in a different way. You sit with your PC, you sit with screens, you sit with tools, whether you knew them or not."*

Excerpt D7: *"The technical part of the exercise was non-ideal, but we were still able to learn. Everyone was included, even though the platform was completely unfamiliar to all our IT staff. They had gotten, I'd say, a crash course in it, and didn't really have the benefit that I had hoped IT staff would get. They became kind of supporting players to the crisis management that actually got the most benefit from the exercise."*

Excerpt D8: *"We've tightened up tremendously on what kind of access you have and don't have. We've tightened the use of administrators, that is...use of shared administrator-accounts have been cut down so that...those who are system administrators use multi-factor authentication."*

Excerpt D9: *"And we have of course continued to work at the system level as well as in relation to [crisis management tool]."*

B.5. Double-Loop Learning: Culture

Excerpt E1: *"We have to pay licenses, we have to pay for that security solution... We don't have that in our budgets yet. That's something we work to provide - or, that I constantly bring up in meetings with the security leader."*

Excerpt E2: *"It's not certain they say yes to it. Even though the politicians also see this with security, they can have completely different priorities in terms of: OK. Should we close a school, or should we... You know."*

Excerpt E3: *"There's no doubt that [the nearby municipalities' incidents], combined with that the municipal director, mayor and the rest of the crisis management...joined the [exercise] and gained increased competence around it, has made it easier for me to get resources prioritized within IT security."*

Excerpt E4: *"Everyone contributes to create vulnerability. So it's important to reach them so that the basic rules we want to have are known by everyone."*

Excerpt E5: *"ICT has always been like this, I think, because it's a bit complex. There was a manager who said to me: 'All the invoices I get from you I just approve, because I understand nothing about what's written on the invoices.'"*

Excerpt E6: *"And then I have told them that I'm not going to do this every single month. You have a job to do yourselves. And I'm not the boss, I'm not the municipal director, so I haven't pursued it any more than some small reminders here and there."*

Excerpt E7: *"It shouldn't take long for management to sit down after a BIA analysis. Because that's the most important, and that's the most important, second most important... To sit down and make priority lists at the application system level... That's holistic work that must be done, which is not just ICT...ninety percent here is actually how the municipality has arranged to make those plans. And ICT shouldn't do that. ICT owns the operational part. And the operational security tasks. And they shouldn't decide that, no, that system is more important than that [other] system. ICT cannot decide that."*

Excerpt E8: *"I think paper exercises often become a bit too superficial. There [at this particular exercise,] you had to go into more detail, as long as everyone was involved and played along."*

Excerpt E9: *"You don't get your pulse up in a paper exercise...I think to have a platform...where you can practice in a safe environment...does something to your feelings, and it does something that you take back to your own organization."*

B.6. Double-Loop Learning: Structure

Excerpt F1: *"Normal structure in this group is that we have a startup meeting, we get a shared situational understanding, we delegate tasks. We take a break until the next meeting, define the next time. We work with tasks and information gathering. New meeting. Shared situational update. Where are we now? What's happening now? Round the table with those affected. We continue building situation pictures. Identify measures. Define a new meeting, have a work period and so on. The way I experienced the exercise, it became one long meeting. That is, we actually didn't get to work."*

Excerpt F2: *"My observation is that the topic and the seriousness of the topic made people lose their heads a bit. So, the calm that we normally have in such handling, which I've now seen several examples of, wasn't there. I thought it was very interesting."*

Excerpt F3: *"Now our exercise was a bit of a slow starter. We used awfully long time in the beginning, and we actually used all of day 1 on the startup meeting."*

Excerpt F4: *"That's one thing I saw that was perhaps the weakest, then. It was the information flow. And we've now handled that by implementing - we use [the crisis management tool] with separate logs. Where they can actually send over information. (...) They get small drips of information, which are selected, and which they choose to send over. Instead of a doomsday prophet that comes in and gives a lecture, where people don't catch all aspects and details because they get it orally and not in writing."*

Excerpt F5: *"Crisis management, even though there are many competent municipal managers within their areas, doesn't have detailed knowledge and grassroots competence, so to speak. Should we pull out the internet cable, or should we leave it in? That's such a concrete question that we're absolutely dependent* *on good advice from IT. What is the consequence if we leave it in, and what is the consequence if we take the chance that it should still be there. And then, the interaction between crisis management and IT is especially important. We didn't have that day one, we had it day two. But that is about structure in the implementation of crisis management. Where we day two had a status meeting every hour, where IT was involved. And otherwise IT basically worked in the data room."*

B.7. Double-Loop Learning: Methods

Excerpt G1: *"Normal structure in this group is that we have a startup meeting, we get a shared situational understanding, we delegate tasks. We take a break until the next meeting, define the next time. We work with tasks and information gathering. New meeting. Shared situational update. Where are we now? What's happening now? Round the table with those affected. We continue building situation pictures. Identify measures. Define a new meeting, have a work period and so on. The way I experienced the exercise, it became one long meeting. That is, we actually didn't get to work."*

Excerpt G2: *"I think they experienced that the crisis unfolded at a faster pace than what they were used to handle. At least the way they normally handle things, those are things like floods, pandemics, right? Things that develop more slowly, but over longer time."*

Excerpt G3: *"I think also that some have reflected that time is important. I think that we who work in public organizations don't always... Things should be evaluated and it should be considered. If you have an incident, then time is essential, and no incident rolls as fast as a cyber incident."*

Excerpt G4: *"For there is that time aspect with incidents that have to do with information security, or ICT security, or for that matter cyber. It is so diffuse, it can take so long. It is not certain you see any immediate effect. It is so, that the one who carries it out, he sits and observes and waits for responses, to get confirmation that what they have done actually works. So it's a bit like that. That time aspect is not understood. They are used to a flood: In the course of 24 hours I have information control, and in the course of 72 hours the situation is over. They forget that time aspect. It's difficult to get them to understand that this is something we might have to endure for months."*

Excerpt G5: *"We see that when we do exercises – or, from studies and training: That you must have an anchoring in management beyond top management, if you are to be able to have any robustness when unwanted incidents occur... We must think even more about somewhat long-term situations, and how you do that with staffing plans, so that you manage to stand in it. For an exercise, it ends when the exercise is finished. But we see from experience, where it has happened, that it can go on for weeks and months."*

Excerpt G6: *"The fact that to manage, for the technical people to communicate in a way that is technically correct, but at the same time provide a picture of cause and effect... I think maybe that's challenging. For this crisis management, they understand intuitively when you talk about a flood, that you must set up a wall there, or that a bridge has collapsed. These are very physical things, so we're used to visualize that. But if you talk about a WAN-link being down, or a hard disk, or a single server... Those are things that – you might as well have talked about components in an engine under the hood."*

Excerpt G7: *"Yes, and it's also a thing that the more stress you are under, the less time (...) you also use to weigh your words. And that's the problem, that those who sit on the other side, the receivers, are hypersensitive to what I call those words that help maximize the crisis. Yes, they are very receptive, but maybe without hearing the whole message."*

Excerpt G8: *"So, we experienced afterwards, at least especially when we started to evaluate it, that [the person] who is responsible for IT spent far too much time to inform the crisis management and answer the crisis management's questions instead of actually work on fixing the incident."*

Excerpt G9: *"And then there's this thing about... How technical can you say something in such situations? That's why it was very good help with that PowerPoint brief that I got help with from [name]. (...) It almost says: Don't talk technically, right? Because people are very good at talking technically, right? But, no! 'That is down. Things don't work. We're working on the matter. That doesn't work, that doesn't work, that works.' I mean, simple and straightforward. So that [brief template] must be a great help, in that sense, when you're going to first have a small brief for management."*

Excerpt G10: *"I clearly state that I can do a little, but how should I make an escalation plan when I* *don't know how important that system is, right? (...) Because you make it based on: Oh, if we are hit here, that results in that, and that results in that..."*

Excerpt G11: *"We have picked out 13 systems that are priority to restore if everything goes black. And then we have simultaneously said that system 14 and beyond, we don't care about that, we'll manage without that. But care system, journal system within care, among others, we must have that. We must know who should receive care during the day, and which medicines they should have, and who we should visit. But it's maybe not equally necessary that the chimney sweeper knows who [s/he] should travel to and sweep the chimney for that day."*

Excerpt G12: *"But that doesn't mean that nothing has happened in the municipality, because we have had many rounds on... How should we continue to run the municipality if we get a cyber attack? Or if the server goes down, or the Internet goes out? So actually, we have done a lot, discussed a lot, had a lot of focus on it, without using the term. (...) So I haven't even learned that term myself, the one you used. But to maintain operations in the municipality when the power goes out - we've talked a lot about that."*

B.8. Double-Loop Learning: Machines

Excerpt H1: *"We might be able to hire a person, we might be able to pay him for a couple of years, and then he would get bored and leave. Because it's a very shallow pond, and there are very many fishing lines out there. And such a person will never be somewhere where he's not challenged. A municipality is unfortunately not that place."*

Excerpt H2: *"What is a long-term challenge, is to achieve an organization that can monitor 24-7... But it's about being prepared, so that it doesn't take a long time when there's an unwanted incident."*

Excerpt H3: *"Yes, because I think an incident with us would quickly be... There are two parts we care about: Finding out what happened? And how we should restore normal operations? With a small ICT department in a small organization, it's demanding. It's many of the same people who have to do the job. We would have to bring in external people, immediately, if we had such an incident."*

Excerpt H4: *"I was very happy that we got an agreement with [company name] now. Because one of my big nightmare scenarios was that we had no supplier of support services from any kind of company."*

Excerpt H5: *"The fact that we would have such an exercise initiated that we started to work more strategically with it, and made several plans that we didn't have initially. It has also resulted in that we now have entered into an agreement with [company name] regarding security monitoring."*

B.9. Triple-Loop Learning: Culture

Excerpt I1: *"If we say for example a system like Sosio, which NAV uses, its function is to safeguard the most vulnerable in society. And if that fails, and it doesn't need to fail for long, it can mean that there are people who don't get food, who don't get money. And that will have a social consequence in addition."*

Excerpt I2: *"After two years in a municipality, I have never encountered an organization that has higher workload, fewer resources and is so understaffed. And that makes everything a priority... They have to focus to keep their head above water. Simply doing what needs to be solved. Legal requirements trump what would have been nice to implement."*

Excerpt I3: *"That local knowledge and creativity... I can call him, the caretaker, he's very good at such things. He can take that responsibility. I think that's a very good thing to have in an emergency situation."*

Excerpt I4: *"That interplay when you have an emergency situation, that is what makes you good or bad, I think. That it is the right people, who know the business well and who know what they can contribute to doing."*

B.10. Triple-Loop Learning: Structure

Excerpt J1: *"That's why we now realized that we must have... We now have an IRT leader, and the IT manager, who communicate between themselves. And then the IT manager must weigh the words that go in, or that is, the information he contributes."*

Excerpt J2: *"That's one thing I saw that was perhaps the weakest, then. It was the information flow. And we've now handled that by implementing - we use [the crisis management tool] with separate logs. Where they can actually send over information. (...) They get small drips of information, which are selected, and which they choose to send over. Instead of a doomsday prophet that comes in and gives a lecture, where people don't catch all aspects and details because they get it orally and not in writing."*

Excerpt J3: *"I remember that when we established the logging function for the IT group, the connection became better. It was almost completely necessary. (...) So the contact between crisis management and the IT group was dependent on that logging function. And in that way, it became a translator function, or a mediator between the two groups that was completely necessary."*

Excerpt J4: *"I could have liked to see the scope of such an exercise change a bit... But what if we look at what would happen if the region is attacked, the county, or actually the whole country. What then?"*

Excerpt J5: *"We are completely dependent on achieving regional cooperation, we wouldn't have had a chance to manage it alone as a small municipality."*

B.11. Triple-Loop Learning: Methods

Excerpt K1: *"Because you have to use some creativity when you're in a crisis management... Either it's damage limiting, or to find a solution because things can't go exactly as they do in daily life."*

Excerpt K2: *"The lectures were actually very good. The problem was that it went right over the heads of everyone who didn't have special insight into that stuff."*

Excerpt K3: *"This could have been given drip-wise in advance, and preferably better adapted...recorded as webinars, and distributed in advance, that people could watch when it suited them."*

Excerpt K4: *"So there is a huge span in that competence among the course participants. And the setup, that walkthrough, was probably adapted more to experienced data users and people with a smidgen of competence within IT security, and not so much for a municipal director with the overall perspective."*

Excerpt K5: *"I thought that was very useful. There we got...in a way, that was when we got the pegs in place, and got reality-oriented with regard to: What is this about? What are the threats? What is the risk? What are the scenarios? So it was through those lectures that we understood...and maybe... If we had had those lectures... Maybe those lectures should have been in November 23, then I think the preparation phase would have been much, much better."*

Excerpt K6: *"I think it's very important to get people out of their buildings. That was very good. (...) We struggle to keep the attention of managers. That's because they drown in work. (...)So to free them from their workplace, that's alpha and omega to get their attention."*

Excerpt K7: *"(...) I think that might have been one of the key factors for us actually managing it. Also because it's much easier not to be so disturbed by all sorts of other daily operations. If we had sat here physically at the town hall, and then we would have a fifteen-minute break just to stretch our legs. Then you meet someone in the hallway who wonders about this and that, and then this and that happens, and then it happens so quickly that it becomes fragmented, and then it suddenly doesn't become so realistic anymore either."*

Excerpt K8: *"It was actually surprisingly easy to live into what was explained as a scenario. So I think it went surprisingly well, and that almost everyone bought into the incident, that it actually had happened."*

Excerpt K9: *"I think exercises... I think there's a greater danger that exercises can become too calm. You should put yourself in a position to solve a real situation. And if the blood-pump goes a bit faster when it's real, then it's not bad that it goes a bit faster when it's an exercise too. That we get to feel, and get to try out, yes: What do we do then? When we get stressed?"*

Excerpt K10: *"I experienced maybe the preparation as... What shall we say, a bit... A bit difficult to take in because I... It wasn't quite clear to me. We had some tasks, and we had some meetings, and we had something we were supposed to send in, and then... It actually took a very long time before I actually understood, what was it we were prepared for? If we had had that lecture... Maybe those lectures should have been in November 23, then I think the preparation phase would have been much, much better."*

B.12. Triple-Loop Learning: Machines

Excerpt L1: *”With a small ICT department in a small organization, it’s demanding... We would have to bring in external people, immediately, if we have such an incident. I would never spend time to investigate what had happened. We would have to hire people to do that.”*

Excerpt L2: *”We are dependent on external actors... We might be able to hire a person, we might be able to pay him for a couple of years, and then he would get bored and leave. Because it’s a very shallow pond, and there are very many fishing lines out there.”*

Excerpt L3: *”We have chosen to spread things in different directions... So it’s a strategy to go out to the cloud with most things.”*