Human Factors in Cybersecurity, Vol. 91, 2023, 111–120
https://doi.org/10.54941/ahfe1003725

Training the Trainers for Cybersecurity Exercises - Developing EXCON-Teams

Grethe Østby, Bjørn-Emil Sælebø, and Stewart James Kowalski

Norwegian University of Science and Technology, Gjøvik, Norway

ABSTRACT

In recent years there has been a large increase in advanced computer attacks targeting Norwegian authorities and businesses. At the same time there is a great shortage of trained and qualified personnel within cyber- and information security. To fill this demand supply gap there has been an increased focus to educate new personnel through exercises and training. Running the training and exercises in a realistic and safe environment is a demanding task, which requires a well-trained Exercise Control (EXCON) team. In this paper we present results from in-depth interviews which were conducted with information security and/or exercise experts from different Norwegian organizations with relevant EXCON experience and suggest a future train-the trainer concept to meet the challenges found in the study. The result from the research shows that the development of exercise control teams is not prioritized by organizations, and not given time or resources for education or team development. Being part of an exercise control teams is a side job where organizations mostly rely on hiring external experts. Another key finding in this research is the importance of exercise planning competence amongst the exercise control team, for the exercises to be successfully executed. Results from the study also shows that a core team of experts is necessary to continuously improve exercises, and that there is a need for these experts to participate in the preparation for exercises.

Keywords: Train-the-trainer, Information security, Cyber security, Training, Exercises, Crisis management

INTRODUCTION

In recent years there has been a large increase in advanced computer attacks targeting Norwegian authorities and businesses (PST, 2021). At the same time there is a great shortage of trained and qualified personnel within cyber- and information security (Cisco, 2018). To fill this demand supply gap there has been an increased focus to educate new personnel through exercises and training (Nikolova, 2017). To meet this increased demand the Norwegian government in cooperation with several private and public organizations and academia established the Norwegian Cyber Range (NCR) in 2018 (NTNU, 2019). NCR is an arena for testing, training, and exercising in cyber- and information security (NTNU, 2019). Running the training and exercises in a realistic and safe environment is a demanding task, which requires a well-trained Exercise Control (EXCON) team.

In a military context NATO's Bilateral Strategic Command (BI-SC) Directive 75-003 – Collective Training and Evaluation appendix H;" Roles and responsibilities of the exercise control (EXCON)" (NATO, 2013), provides a clear plan for how to establish an EXCON team that can properly direct and control an exercise (NATO, 2013, pg. 166). In addition, Østby et al. have suggested how to build an EXCON team to train public emergency organizations (Østby et al., 2019). Neither of these specify how the EXCON-team itself should be trained.

In their Comprehensive ICT risks report of 2015 NSM states the need for more cyber- and information security competence and training as an important tool to acquire and implement new knowledge and skills to create a strong and resilient cyber- and information security organizations (NSM, 2015), and we suggest a continuous focus to train and to build competent EXCON-teams to run the exercises needed in the society.

In this paper we present results from in-depth interviews which were conducted with information security and/or exercise experts from different Norwegian organizations with relevant EXCON experience and suggest a future train-the trainer concept to meet the challenges found in the study.

After this introduction we present some background material and relevant literature before we outline the research approach in the study. After presenting the methods, we present the findings and thematic analysis before we conclude and suggest future research on the topic at hand.

BACKGROUND AND RELEVANT LITERATURE

Cyber security exercises have proven to be a highly effective mechanism to provide information security awareness and uncover gaps in information security plans, procedures, and policies (Furtună et al., 2010). Many initiatives to train and educate personnel through exercises to gain competence and skills within information security are supported, and as a result, exercises conducted within the field of cyber- and information security in Europe represented over 40% of all global exercises in Europe in 2015 (Nikolova, 2017).

In order to establish an EXCON team that function well there are many different factors that must be considered, both regarding different types of exercise, the organization to be trained, the EXCON-team's area of competence, education, and diversity to meet the goals of the exercise (Østby et al., 2019). Cyber-attacks may affect most parts of an organization (Østby & Kowalski, 2022), from the management down to the system engineers, and cyber- and information security exercises must take this into consideration to be effective and efficient, which would be the core responsibility of the EXCON-team.

To successfully plan and execute an exercise can be a challenge, and it is vital skills within an EXCON team. To meet this skill demand there is a need of structured procedures and methods. One example of such procedures is the mentioned NATO's Bilateral Strategic Command (BI-SC) Directive 75-003 – Collective Training and Evaluation (NATO, 2013), where appendix H;"

Roles and responsibilities of the exercise control (EXCON)" is of relevance (NATO, 2013).

Other useful guidelines are the Norwegian Directorate for Civil Protection (DSB)'s method booklets, and specifically the "Guidelines in planning, implementation and evaluation of exercises" (DSB, 2016). The DSB guideline focuses on how to conduct training and exercises of different sizes and types (DSB, 2016).

In addition, the European Union Agency for Cybersecurity (ENISA) describes different roles that must be performed during the life cycle of an exercise: "Organizer, Planner, Participant, EXCON team, Facilitator or moderator, Observer, and Evaluator" (ENISA, 2009).

To build an EXCON team for cyber- and information security exercises, one should firstly consider what organization, and therein layers in the organization, one is about to train before one decide the team (Østby et al., 2019). Experiences from full-scaled exercises and computer assisted exercises also shows that some exercises like full-scaled exercises can have a complex form which requires high number of recourses, while computer assisted exercises (CAX) are more effective in terms of recourses (Nikolova, 2017). CAX has also been proven highly flexible with the possibility to attend from different places in the world (Zinca & Bârsan, 2021). From experiences at the NCR, we have however found that the number of EXCON-participants in the CAX-exercises has outnumbered the number of EXCON-participants in the full-scaled exercises executed.

We do however suggest that EXCON teams also should get targeted training to better be prepared for the exercises. Especially, to have proper knowledge and skills to give the participants the best possible learning experiences from the exercise. Learning can be defined as "something that happens, which leads to lasting changes in a person who learn" (Illeris, 2012). Learning can both be in terms of new knowledge or skills, and it may be learning in both a positive and a negative sense.

Illeris also defines two directions within the learning process: The acquisition process and the interaction process (Illeris, 2012). The process is illustrated in Figure 1, and consist of three dimensions: content, incentive, and interaction. The model is based on an understanding that the three dimensions are dependent on and influencing each other.

'Content' is defined as "knowledge, understanding and skills", 'incentive' as "motivation, emotions and will", and 'interaction' as "communication, action, and cooperation" (Illeris, 2012).

An important dimension of the learning process is whether the learning process is distributed in-between the organizational members (Argote & Miron-Spektor, 2011). Organizational learning can be described as "Changes in the organization's knowledge that occurs because of acquired experience" (Argote & Miron-Spektor, 2011). In compariason to Illeris dimensions of learning, also the organizational learning happens in a context, both to the internal organizational and to the environmental context which the organization is embedded into (Argote & Miron-Spektor, 2011). The internal context of an organization includes characteristic such as structure, culture, goals, technology, strategy, etc., while environmental context is element outside the

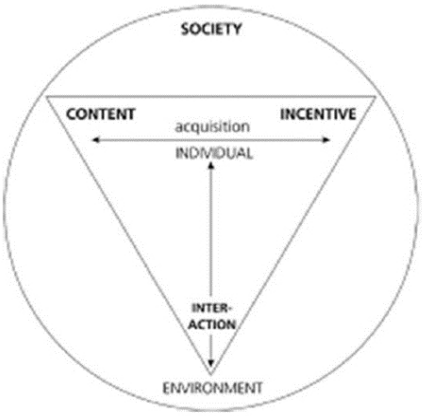

Figure 1: Illeris' three dimensions of learning (Illeris, 2012).

organization, and for an EXCON team this can be the training audience, exercise type, other institutions, or partners (Argote & Miron-Spektor, 2011).

Organizational learning is a continues process that happens over time. It begins with individual, team, or organizational experience, all which contribute to the organizational learning (Argote & Miron-Spektor, 2011). Experience can also be acquired directly by the organization, or indirectly, which for an EXCON team could be to acquire experience by observe other cyber- and information security exercises. Within an organization that has a memory system that are well developed the members can specialize in acquire different pieces of information and knowledge, for then to distribute the knowledge in the organization (Weick & Roberts, 1993).

> "The collective mind that emerges during the interrelating of an activity system is more developed and more capable of intelligent action the more heedfully that interrelating is done." (Weick & Roberts, 1993).

Knowledge retention is whether acquired knowledge is perceived and reused in the organizational memory over time (Argote & Miron-Spektor, 2011). High turnover in an organization can often affect the retention of knowledge (Argote & Miron-Spektor, 2011). However, research shows that organizations that are highly structured, hierarchical, and where the members follow, organizational processes are better equipped to keep knowledge even when the turnover is high (Argote & Miron-Spektor, 2011). This can also apply to EXCON teams with a 'natural' high turnover, where a structured (or as we suggest – a core team of) EXCON management, with good routines and procedures, help retain knowledge. This is also adaptable to how the knowledge in high turnover organizations (like the EXCON-teams) is transferred, that is, if it is transferred as tacit knowledge or scientific competence, or as referred to by Weick & Roberts: habitual or heedfully actions.

> "In heedful performance, the agent is still learning. Furthermore, heedful performance is the outcome of training and experience that weave together thinking, feeling, and willing. Habitual performance is the outcome of drill and repetition." (Weick & Roberts, 1993).

Knowledge transfer is when the organization obtain knowledge and learn indirectly from others experience, as well as directly by own experience. We do however suggest that also for EXCON-teams heedful training and scientific competence should be provided.

There are several models and framework that describes how to train and develop instructors and teachers. One process used to train nurse educators to use simulation effectively is a "Train-the-Trainer" (TTT) process as presented by Lane & Mitchell (2013). The TTT process focuses on three different stages, firstly a Champion identification stage, secondly a Champion development, and finally a Champion integration (Lane & Mitchell, 2013).

The strong side about the Lane & Mitchell TTT process is that it is a framework that aims at training personnel to become teachers (or in our case, trainers) in their own organization. Another strength of this process is that it is based on the heedful performance, recognizing that not everybody has tacit knowledge or skills to be a great leader or teacher. By selecting personnel based on their personal characteristics and interest at an early stage, an organization can identify and develop personnel who are suitable to fill positions in an EXCON team, and also to integrate the team-members step-by-step based on their gained knowledge and skills.

RESEARCH APPROACH

To address how EXCON-teams can gain relevant competence we approached the challenge by what can be referred to as an inductive approach, using case-studies to observe the phenomenon. The inductivist approach starts by first observing a phenomenon and then generalizing about the phenomenon which leads to theories that can be falsified or validated (Kowalski, 1994). Semi-structured interviews were executed with experienced experts in exercise control within either or both cyber-and information security or crisis management.

In qualitative studies one tries to acquire as much information as possible from a limited number and carefully selected informants (Johannessen et al., 2021). Thematic analysis can be exploratory in their nature (Saunders et al., 2012) and was therefore chosen to analyse the transcripted interviews. "An exploratory study is a valuable means to ask open questions to discover what is happening and gain insights about a topic of interest" (Saunders et al., 2012). Explanatory analysis from the EXCON-teams' evaluations were added to establish causal relationships between the exercise goals and the learning outcomes – from the EXCON-team perspective. "Studies that establish causal relationships between variables may be termed explanatory research" (Saunders et al., 2012).

FINDINGS AND ANALYSIS

A common feature for all the informants in the study was that they all highlight the importance of exercise planning and an early involvement from EXCON in the planning of the exercise. It was also a unison view among all the informants that good situational awareness amongst the EXCON

team is highly important in advance, during and after the exercise. How EXCON-teams were trained and educated within the different organizations were answered from many questions, and several sub-themes were outed as important, that being different dependencies as e.g., available resources, priority (being a 'side-job'), and, learning by doing. All the informants agreed that to understand both the social and technical aspects is important for an EXCON team, and there was also a common understanding amongst three of the informants that the human factor is mostly trained (and focused on) higher up in the organization in-between the decision makers. Several of the informants informs that they use literature in operational planning when planning and executing an exercise. Important literature mentioned by the informants from the military is the NATO's collective training and exercise directive (BI-SC 075-003), and the Norwegian militaries plan and decision-making process. To design an EXCON-team, resources were outed as a limiting factor when discussing optimal output for training the EXCON team. The informants explained that any aspects and disciplines implemented in the exercises greatly affects how demanding it is to follow up, that is, how the level and type of events greatly effects the composition of the EXCON team. the informants describe the importance of EXCON team members knowing each other, and to understand each other's area of expertise, strength, and weaknesses. Serval of the informants has experienced difficulties when it comes to communication between team members with different technical background. This in terms of use of technical terms and to understand the technical limitation. The informants expressed the importance of evaluation to properly develop an EXCON team. However, as with other factors aimed at developing EXCON teams, most of the informants had experienced that to evaluate EXCON it is not prioritized. Again, it mostly came down to lack of time, resources, and risk reward. These different themes were categorized in 4 main themes and several sub-categories, which is presented in Figure 2.

From the first sub-category 'involvement in planning processes' it was found that, 1) exercise intentions and goals, 2) participation in planning

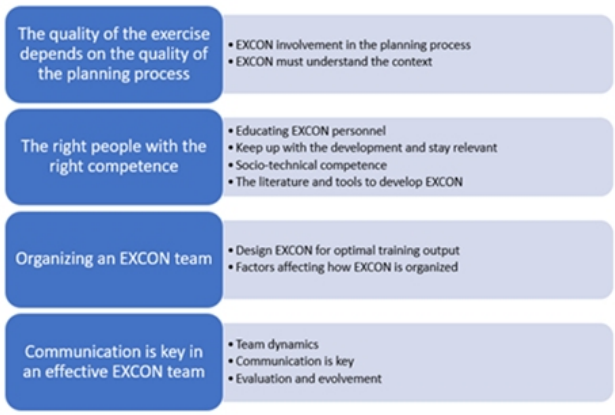

Figure 2: Themes and sub-categories.

process, 4) scenario development, and 5) case development, were essentials to succeed in the planning process. One of the informants describes it as

> "Often it is those who are most involved in the planning process prior to the exercise who get roles in the EXCON-team, this is due to the fact that it is very important to have good control of the scenario and what the exercise should involve to able to do exercise control".

From the second sub-category 'understanding the context' it was found that 1) situation awareness, 2) understand the cyber domain, 3) understand your training audience, 4) understand the training objective, and 5) understand the organization, were of importance to understand the context.

> "First of all, I think that the competence must be present in the EXCON team, because if you first analyze what you want to exercise and have exercise goals at the other end, the EXCON team must be designed so that you can achieve those goals for the practitioners."

From the third sub-category 'education EXCON personnel', it was found that 1) education depends on resources, 2) learning by doing is the most common way to learn about exercise control, 3) train-the-trainer is executed 'on time', 4) exercise and planning courses exists, but are not necessarily providing role-training for exercise control participants, and 5) the EXCON-manager doesn't need to be an expert. To 'keep up with the development and stay relevant', it was suggested to 1) be hungry for new knowledge, and that 2) the competence can be hired.

> "(..) you have experts that is like "I just learned something new there", where is if you are employing experts that just think they know everything maybe they're not so willing to learn and so you need to have experts that are humble"

'Socio-technical knowledge' was seen as important from all participants, and comments like

> "When it comes to including the social consequences during exercises, this is something that is trained at a strategic and higher tactical level. While at the lower level there is more focus on the technical. The social is not important there"

and

> "We are the ones opening up those phishing emails and so the socio is incredibly important, yeah social engineering in there and it's only going to be more and more social engineering because our technology is getting better and better and our ability to digital detection is getting better and better so access becomes harder, but we are still the soft target."

lead us to understand that 1) the human factor gets down prioritized, 2) you need to think 'so what' for yourself, as 3) humans are often the target.

'Known literature' amongst the participants were mainly the NATO exercise directive and the NATO CAX guidelines. To 'Design EXCON for optimal training output' it was found that 1) (also for this one) that it is

dependent on available resources, and 2) that there is no such thing as a perfect template today.

> "(..) Access to people with the right competence is important and is always a limited factor, especially on the technical side access to competent people limits the level of complexity of the events."

'Factors that affect how EXCON is organized' were found to be 1) complexity and 2) exercise type.

> "One should avoid organizing an EXCON team the same every time, one must be able to adapt the organization to the type of exercise and what to train. Many people go for a fixed organization, it does not necessarily fit as well on the tabletop as on larger exercises"

> "And too often we just send people on exercise because he's available and it doesn't work. It doesn't work. EXCON teams need to train together."

As communications were one of the main findings from the interviews, 'team dynamics' where 1) the EXCON-team were desired to be well grounded, 2) time for team development, 3) defined roles, and 4) a hands-on leader, would be essentials to get good communication. 'Key communication' skills wanted were 1) a focused EXCON-leader, and 2) speak the same language (also being same technical language). It was also desired to 'evaluate and evolve' to 1) one must commit to evaluation and 2) measure the EXCON teams' performance.

An overview of the findings is presented in Figure 3.

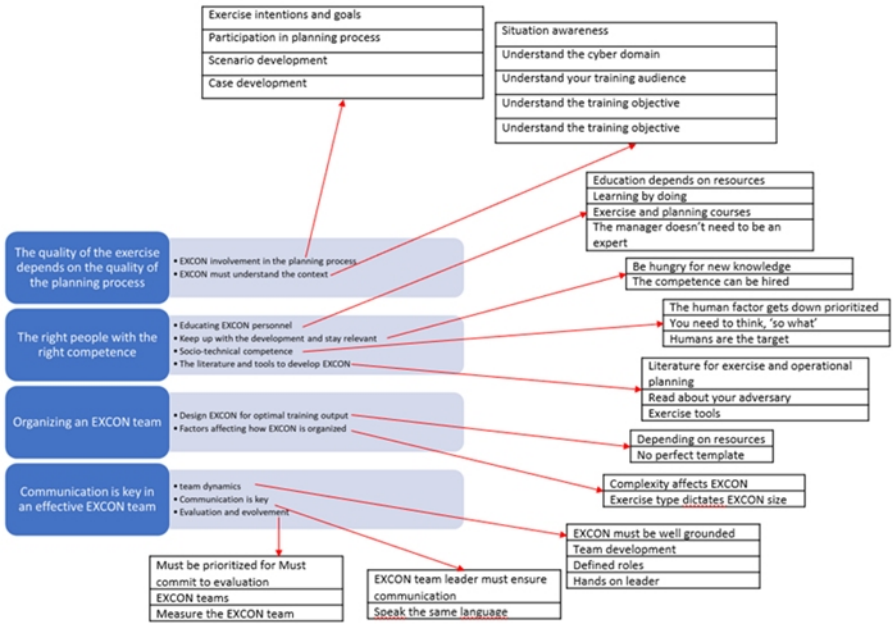

Figure 3: Thematic findings.

CONCLUSION AND FUTURE RESEARCH

The result from the research shows that the development of exercise control teams is not prioritized by organizations, and not given time or resources for education or team development. Being part of an exercise control teams is a side job where organizations mostly rely on hiring external experts. Another key finding in this research is the importance of exercise planning competence amongst the exercise control team, for the exercises to be successfully executed. Results also shows that a core team of experts is necessary to continuously improve the exercises, and that there is a need for these experts to participate in the preparation for exercises.

We suggest that these experts also should be the core members that both participate in the preparation of the exercises, but also are the ones to train other new potential 'champions' that could participate in EXCON-teams. Next, we suggest that a cyber-range that will be dependent of different types of 'champions' would need a pool of trained EXCON-members that can support the core experts dependent on what type of exercise that will be executed. This suggestion can be visualized as in Figure 4.

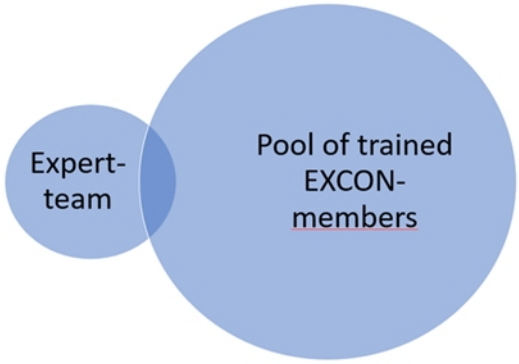

Figure 4: Pool of trained EXCON-members.

As found in Lane & Mitchell (2013), the three-step process to create and unofficial role of 'champions' in the training organization can become a solution for any cyber-range, and future research is needed to see if it is more effective to create and unofficial role of 'champion' from a pool compared to create a permit staff function of experts.

ACKNOWLEDGMENT

The authors would like to acknowledge those who participated in the interviews.

REFERENCES

Argote, L., & Miron-Spektor, E. (2011). Organizational learning: From experience to knowledge. *Organization Science*, *22*(5), 1123–1137. https://doi.org/10.1287/orsc.1100.0621

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

ENISA. (2009). *Good Practice Guide on National Exercises*. 80. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber_exercises

Furtună, A., Patriciu, V. V., & Bica, I. (2010). A structured approach for implementing cyber security exercises. *2010 8th International Conference on Communications, COMM 2010*, 415–418. https://doi.org/10.1109/ICCOMM.2010.5509123

Illeris, K. (2012). *Læring*. Gyldendal akademisk.

Lane, A. J., & Mitchell, C. G. (2013). Using a train-the-trainer model to prepare educators for simulation instruction. *Journal of Continuing Education in Nursing*, *44*(7), 313–317. https://doi.org/10.3928/00220124-20130515-33

Johannessen, A., Tufte, P. A., & Christoffersen, L. (2021). Introduksjon til samfunnsvitenskapelig metode. Akademika.

Kowalski, S. (1994). IT Insecurity: A Multidisiplinary Inquiry. Stockholm University. Saunders, M., Lewis, P., & Thornhill, A. (2012). Research Methods for Business Students (6th ed.). https://gibsoncollege.edu.et/wp-content/uploads/2022/01/Research-Methods-for-Business-Students-by-Mark-Saunders-Philip-Lewis-Adrian-Thornhill-z-lib.org-1.pdf

Nasjonal trusselvurdering 2021, (2021). https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/

NATO. (2013). *Resilient e-Communications Networks Good Practice Guide on National Exercises Enhancing the Resilience of Public Communications Networks Good Practice Guide on Exercises 2 Good Practice Guide on National Exercises*. https://www.enisa.europa.eu/act/res

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

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

NSM. (2015). Risiko 2015, Nasjonal sikkerhetsmyndighet. https://nsm.no/getfile.php/133732-1592916559/NSM/Filer/Dokumenter/Rapporter/nsm_risiko_2015-web.pdf.

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

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

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

Weick, K. E., & Roberts, K. H. (1993). Collective Mind in Organizations: Heedful Interrelating on Flight Decks. In *Quarterly* (Vol. 38, Issue 3). https://www.jstor.org/stable/pdf/2393372.pdf?refreqid=excelsior%3Ab1322493c2143002f6e7180cb57b5062&ab_segments=&origin=&acceptTC=1

Zinca, D.-I., & Bârsan, G. (2021). Planning and Conducting Computer Assisted Exercises During a Pandemic. *Land Forces Academy Review*, *26*(1), 76–86. https://doi.org/10.2478/raft-2021-0012