International Journal of Safety and Security Engineering
Vol. 12, No. 3, June, 2022, pp. 299-310
Journal homepage: http://iieta.org/journals/ijsse

Cybersecurity Training in Norwegian Critical Infrastructure Companies

Nabin Chowdhury[1*], Espen Nystad[2], Kine Reegård[2], Vasileios Gkioulos[1]

[1] NTNU, Teknologivegen 22, 2815 Gjøvik, Norway
[2] IFE, Os Alle´5, 1777 Halden, Norway

Corresponding Author Email: nabin.chowdhury@ntnu.no

https://doi.org/10.18280/ijsse.120304

Received: 16 June 2021
Accepted: 25 April 2022

Keywords:
state of practice, cybersecurity, awareness, training, critical infrastructure (CI), interview, questionnaire

ABSTRACT

Human preparedness is a critical aspect of critical infrastructure (CI) cybersecurity. Many efforts, including educational curricula and training programs, have been taken at both national and company level to ensure human preparedness in CI incident response. These efforts are usually based on corporate requirements or external guidelines and policies. However, the best practices recommended for these efforts in the literature differ significantly from the measures implemented in CI companies. For this reason, we compared state of practice in cybersecurity awareness and training in selected CI companies with the recommendations in literature, aiming to identify the areas that CI companies need to increase efforts for further security implementations. Specifically, we conducted interviews (n=7) and sent out questionnaires to cybersecurity personnel (n=11) in different CI sectors of Norway. The collected data were analyzed to establish the commonalities, differences, and areas of concern among the interviewees, with respect to certain critical attributes. All Norwegian companies involved in the study offered some type of awareness or training activities to their employees, but these activities varied greatly in the level of maturity. Besides, we noted several limitations in methods and contents. According to many participants, the team skills, communication skills, and managerial skills were often inadequately developed. Additional limitations in delivery methods were noticed, too. Finally, we suggested the solutions from the best practices in the literature, and pointed out the areas where the literature has not provided effective measures.

1. INTRODUCTION

In many developed countries today, the national and economic security hinges on the reliable functioning of critical Infrastructure (CI). Successful cyberattacks against CI may cause considerable economic and reputational damages to companies, countries, and the public. In recent years, there has been an ever-increasing risk of cyber-attacks to digital systems that enable monitoring and control of CI. To deal with the risk, extra focus should be paid onto access control, training of personnel and handling of insider threat [1].

At present, many successful cyber-attacks target corporate personnel, and take advantage of the lack of human preparedness, rather than exploit system or application-level vulnerabilities [2, 3]. In Norway, business managers are increasingly worried about cybercrimes, and experiencing more frequent cyberattacks. The majority of these cyberattacks use social manipulation techniques. 67% of all Norwegian business managers consider employees' unconscious actions as a threat to their operations [4].

Several recent examples of cyberattacks on Norwegian companies and institutions have brought attention to the issue of cybersecurity. Norfund, a government-owned investment fund for developing countries, was victimized by a digital attack, which resulted in a loss of 10 million USD. The attackers gained access to Norfund's email system, and manipulated email communication to transfer money to their account [5]. Hydro, an energy and aluminum producer, was subject to a ransomware attack that had significant operational and financial impacts. Started in a factory in the United States (US), the attack spread to the other parts of the company around the world. The cost of the attack was estimated to 550-650 million NOK (70 million USD) [6, 7]. It is unknown how Hydro's systems were infected, but clicking on links or opening attachments in emails was reported to be the most common way for the ransomware to spread [8]. The above attacks clearly demonstrate the need to focus on human aspects and behavior to ensure CI cybersecurity.

Winnefeld Jr. et al. [9] summarized the lessons learned from the US military: "The clear lesson here is that people matter as much as, if not more than, technology. (Technology, in fact, can create a false sense of security.) Cyber defenders need to create "high-reliability organizations"— by building an exceptional culture of high performance that consistently minimizes risk." The understanding that cybersecurity is about comprehensive and systematic risk management is echoed in best practice frameworks, such as the NIST Cybersecurity Framework [10], and the ENISA National Cyber Security Strategies Implementation Guide.

Humans can both pose a risk to cybersecurity in the form of human errors, and suppress the success and consequences of attacks through preventive behavior, responses, and recovery actions. Therefore, best practice frameworks need to focus on the workforce and cybersecurity culture of organizations, as well as CI. Prominent organizations in cybersecurity (e.g., NIST, and ENISA) and government departments (e.g., US

Department of Energy, and Norwegian National Security Authority) emphasize the need to ensure a "cybersecure" workforce, and provide recommendations and guidelines for cybersecurity assurance. Similarly, a plethora of research in cyber and information security have recommended the contents of competence development efforts [10-13], and the form or method of their delivery [14, 15].

In contrast, far less is known of how CI perceives and addresses its needs for developing cybersecurity competence. There is a serious lack of research into the details about cybersecurity awareness and training for companies, such as the trainees, the training contents, the training delivery methods, etc. Knowing these details helps to learn about the latest measures of cybersecurity preparedness, and to compare them with the best practices recommended in the literature. On this basis, it is possible to develop more effective measures for comprehensive training of cybersecurity skills, and identify the areas where the literature has not provided effective measures.

To contribute to the current research efforts in human preparedness and the training of cybersecurity, this paper overviews the awareness and training offerings in the selected Norwegian CI companies, and compares these offerings to the recommendations in the literature. The research data were collected via interviews and questionnaires from cybersecurity personnel in Norwegian CI companies. These companies operate in sectors like transportation, financial, health care, and energy, or provide services to other CI companies.

The remainder of this paper is organized as follows: Section 2 summarizes the best practices for human preparedness in cybersecurity; Section 3 reviews the related literature; Section 4 details the methodology of the questionnaires and interviews, and introduces how to extract and analyze the collected data; Through data analysis, Section 5 reveals the state-of-practice in cybersecurity awareness and training offerings of Norwegian CI companies; Section 6 compares the cybersecurity training offerings of the selected companies with the recommended measures in the literature, aiming to evaluate these offerings, and identify their gaps and limitations; Section 7 sums up the findings, and provides the directions for future research.

2. BEST PRACTICES

As previously stated, humans are among the greatest security vulnerabilities of CIs. The lack of awareness and training are a major cause of many successful attacks against CI. With the continuous advancement of social engineering techniques, attackers often directly target personnel to get access to confidential data [16]. To mitigate this threat, cybersecurity awareness and training activities have been highlighted both at national level and company level.

Before further analysis, it is important to clarify the distinction between cybersecurity awareness and training. Cybersecurity awareness refers to the level of appreciation, understanding or knowledge of cybersecurity or information security [17]. The common activities to enhance cybersecurity awareness include awareness campaigns [18], educational activities [18-20], and distributing informative documents via mail, posters, or other means [18, 20]. Meanwhile, cybersecurity training aims to develop participants' cybersecurity skills and competences through activities like classroom teaching, e-learning courses, game-based training, and simulation-based exercises [21]. Sometimes, the activities for raising awareness may coincide with basic activities of cybersecurity training. However, the mastery of advanced knowledge, skills and abilities (KSA) requires specifically designed training activities.

Chowdhury and Gkioulos [22] summarized and categorized the key skills and competences of CI cybersecurity personnel recommended in the literature, including the guidance provided by the Workforce Framework for Cybersecurity (NICE). Tables 1 and 2 present the main categories identified by Chowdhury and Gkioulos [22].

Table 1. Mapping of technical and soft skills and competences for CI protection

Technical skills	Soft skills
1.Understanding of digital security concepts; 2.Understanding of evolving threats; 3.Understanding of attack intelligence; 4.Penetration testing skills; 5.Cryptology knowledge; 6.Software and hardware skills; 7.Network security skills; 8.Computer forensics skills; 9.Programming skills; 10.Data analytics skills; 11.Information security skills; 12.Wireless security skills; 13.Proficiency of intrusion detection tools	1.Information sharing and communications; 2.Public speaking and presentation skills; 3.Situational awareness; 4.Cognitive and behavior analysis; 5.Ability to work independently; 6.Trust management; 7.Teamwork; 8.Motivation; 9.Time management; 10.Networking; 11.Confidence; 12.Work habits

Table 2. Mapping of implementation and management skills and competences for CI protection

Implementation skills	Management skills
1.Threat and vulnerability assessment and management; 2.Event and incident response; 3.Continuity of operations	1.Risk management; 2.Identity and access management; 3.Asset, change, and configuration management; 4.System administration; 5.Workforce management; 6.Cybersecurity program management; 7.Supply chain and external dependencies management; 8.Evaluation of policies effectiveness; 9.Project planning

The NICE framework categorizes the common cybersecurity functions, as well as the specialty areas of cybersecurity work and roles, according to the specific cybersecurity KSAs required. It also sets the requirements on workforce recruitment, education, training, and retention of KSAs, enabling educators to develop appropriate training programs for the workforce [10]. However, several limitations of the framework have been noted in the literature.

Jacob et al. [23] argued that, for cybersecurity roles with a weak technological connection, the NICE framework provides poor job descriptions, inadequate guidance on competences, training, and career, and no predictable outcomes or metrics to determine effectiveness. Additionally, the great granularity of KSAs provided in NICE is insufficient to identify key competences and skills required to develop adaptive

cybersecurity training measures for CI personnel, considering resource management.

Over the years, several educational curricula and cybersecurity training frameworks have emerged to develop the skills and competences listed in Tables 1 and 2. Through a systematic review of the literature, Chowdhury and Gkioulos [21] selected key attributes regarding the contents, design, and development of cybersecurity training offerings. These attributes are enumerated in Table 3.

Table 3. Key attributes regarding the contents, design, and development of cybersecurity training offerings

Requirement	Description
Suitability	Training contents should be appropriate to the target audience in terms of contents, skills, and level of training.
Real-life experience	Training should include hands-on activities, developed to emulate, or simulate real-life scenarios. Such activities should also focus on developing communication and team skills of participants.
Scalability and adaptability	Training should allow for modification, upgrading, and extension of contents, based on the skills and level of knowledge of the target audience, as well as new information on technologies and vulnerabilities.
Accessibility	Training activities should be accessible to all staff that may benefit from such activities, including remote access.
Frequency	Training should be conducted and updated periodically. Progress sessions should be planned to ensure that KSAs of personnel are up-to-par to current standards and recommendations.
Efficiency	Training activities should consider resource constraints of a company (budget, time, and training personnel.)

All the above attributes (Table 3) should be considered before developing training programs.

3. LITERATURE REVIEW

Overall, only a few have investigated the state of practice for cybersecurity training in CI companies. This section reviews their works in details.

Chowdhury and Gkioulos [22] systematically reviewed the literature on the key skills and competences needed by CI personnel. They divided these skills and competences into four categories, namely, technical skills, non-technical soft skills, implementation skills, and managerial skills, noted that non-technical skills are often under-prioritized during cybersecurity training, and called for more research on the relationship between non-technical soft skills and other skills and competences, and how the former may influence the effectiveness of the latter.

Chowdhury and Gkioulos [21] conducted another systematic literature review of cybersecurity training offerings, with the goal of establishing desirable attributes of training, preferred training delivery methods, and evaluation metrics of training effect. Their results show that game-based and simulation-based training techniques are preferable to other, more traditional methods. Of course, the combination of different training methods may yield more effective results. Additionally, in Table 3 were also regarded as desirable, and recommended for training development. Finally, the authors concluded that more research is needed to demonstrate whether integrating advantageous attributes from different delivery methods could produce more comprehensive and effective solutions.

Rahim et al. [24] reviewed all the relevant literature on the state-of-the-art approaches for assessing cybersecurity awareness, and recognized some of the major issues or gaps present in these approaches: (1) Lack of flexible use of multiple methodologies; (2) Imperfect categorization of target audiences; (3) Unsystematic evaluation technique for educational programs in the field of information technology. In conclusion, the authors stressed the importance of enhancing the current cybersecurity awareness programs, with particular focus to those dedicated to the younger generations. Ricci et al. [25] surveyed the interest in cyber threat education among adults. Most respondents of the survey were concerned about cybersecurity threats, and their impacts on everyday life. They also expressed eagerness in participating in cybersecurity training initiatives or education. Nonetheless, time and resource were identified as the constraints on the selection between different types of formative activities, as most respondents were unwilling to spend more than 1.5h for a session and more than 20$ per session.

Mouheb et al. [26] presented and compared existing curriculum design approaches for cybersecurity education. By target, they divided cybersecurity curricula into three classes (education, industry, and government/defense), noticed a potential conflict between cybersecurity curricula in higher education and industry needs. Hands-on skills, which are not emphasized in these curricula, are preferred by industrial entities.

4. METHODOLOGY

To analyze the state-of-the-art and practice of human preparedness and training in cyber security for CI, we collected data through questionnaires and semi-structured interviews on cybersecurity professionals from Norwegian CI companies. A total of 11 questionnaires were answered. Then, six of the respondents, plus an additional organization, were subjected to interviews. All participants play the role of management-level cybersecurity roles in Norwegian CI industries, and take charge of cyber/information security or cyber security training in the company. The selected companies engage in sectors like transportation, financial, health care, and energy, or provide services to other CI companies. All respondents and interviewees were informed about the purpose of the study, and the storage and processing of their data. Due to the small number of respondents, we did not select statistically representative samples of Norwegian CI workers, but chose different companies with 500-4,000 employees from different sectors. The questionnaire survey aims to summarize the current and planned initiatives for cybersecurity competence in the CI companies. Eight questions were designed concerning the initiatives implemented in the organization to improve general cybersecurity and enhance specific cybersecurity competence, the need for further improvement in cybersecurity competence, the update frequency of cybersecurity competence initiatives,

as well as the planned initiatives for cybersecurity competence improvement. A respondent can choose between multiple answers for each question, or fill in his/her own answer.

The goal of the interviews is to gain insights into the cybersecurity awareness and training measures being adopted in different sectors of Norwegian CI, identify the defects of these measures, and summarize the company-level plans to tackle these defects.

With the aid of videoconferencing software, the interviews were conducted digitally in sessions ranging from 45min to 1.5h. Each interview consists of a group call involving one interviewee and two or three interviewers, based on availability. During each session, interview notes were collected separately by all interviewers. Later, the notes were integrated and shared with interviewee, to produce an agreed final report. The data reported from the interviews were subsequently modified to remove any information that may disclose the identity of either the interviewees or their companies. Every interview was conducted in line with existing standards for semi-structured interviews [27] to minimize biases (interviewer bias, confirmation bias, etc.), and to ensure the neutral reporting of both questions and answers. The participants' own reflections and evaluation of practices were also collected in the last section of the interview, which shed light on companies' internal vision for cybersecurity training and allow for later comparison with literature's recommendations.

The interviews were structured into three main sections, each focusing on specific contents (Table 4).

Table 4. Contents of each section of the interview

Section	Description
Interviewee's background	This section includes questions regarding past and present experiences of the interviewee in cyber security and related fields. Explicit information regarding interviewees and their companies was eliminated for the purpose of nondisclosure.
Cyber security training	This section includes questions regarding training offerings and other procedures adopted by the company for cyber security awareness and training. More specifically, the questions are about the contents, structures, methods, targeted personnel and future implementations.
Further comments	During the last section of the interview, each interviewee was asked to give any additional comments or opinions regarding the status of cyber security training offerings and procedures in his/her company. This may include evaluations of the current training offering, suggestions for future implementations, and discussions of concerns, future threats, as well as any other topics highlighted by the participants.

The attributes in Table 5 were the focus of data collection on training offerings, in reference to the classification of requirements and best practices discussed in Section 2. These attributes were useful for later categorization during the data analysis.

The interview data were analyzed through qualitative content analysis, following the recommendations of Vaismoradi et al. [28]. The data analysis was implemented in three phases: preparation, organizing, and reporting. In the preparation phase, the interview notes were transcribed, and the transcripts were read several times, to gain an overall understanding of the data. In the organization phase, the categories were defined, reviewed, and searched for, and the notes were classified into suitable classes, using deductive coding. In the reporting phase, the results of the previous phases were reported.

The data extracted from the interview were compared to the standards and best practices for cybersecurity training, which were reviewed and summarized in Chowdhury and Gkioulos [21], and further described in Section 2.

The questionnaire and interview questions are provided in the appendices.

Table 5. Key attributes in data collection

Name	Description
Training basis	This attribute refers to the factors that determine the selection of knowledge, competences, recipients, and delivery methods for personnel training. These may include external factors like national or international policies, best practices, and prevalent training offerings, as well as internal factors like internal policies, threats to the infrastructure, etc.
Training recipients	This attribute refers to the targets of different training offerings. Depending on the type of training, the target group may include specific roles or be expanded to the whole personnel.
Training contents	This attribute refers to the knowledge, skills and abilities developed through training sessions. These may be both technical and non-technical in nature.
Delivery methods	This attribute refers to the methods and tools used by the company to train personnel, as well as the methods to evaluate training effectiveness.
Personal concerns and evaluation	This attribute refers to the interviewees' personal insights into the areas that may be lacking, and evaluation of current training offerings and other relevant topics.
Future plans	This attribute refers to the plans proposed by the interviewee or the company, to be adopted in the near future for improving current training offerings.

5. RESULTS

This section provides the results from the questionnaires and interviews. The results were grouped by the topics in Table 3. The questionnaire results were mainly presented in Section 5.3 and Section 5.5. The number of responses in each class for each question was illustrated in figures. The interview data were analyzed based on the categorization of training attributes in Table 3. The data on each attribute were examined independently.

5.1 Implemented cybersecurity initiatives

As shown in Figure 1, the past five years witnessed a high level of implemented cybersecurity initiatives. At least 10 of the 11 organizations invested in technical infrastructure and cybersecurity tools, hired cybersecurity experts, or made changes to ensure cybersecurity. Eight organizations made initiatives in collaboration with other organizations. Nine organizations implemented cybersecurity competence initiatives. In summary, most companies put at least some efforts into cybersecurity competence development, in addition to more technical or organizational initiatives.

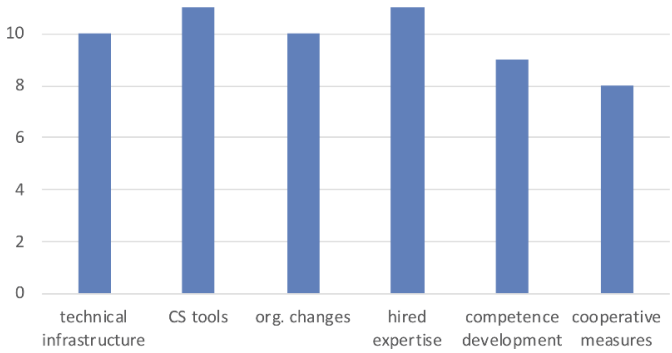

Figure 1. Number of cybersecurity initiatives implemented by the Norwegian companies over the past 5 years

5.2 Training basis

When it comes to the training basis, several criteria for development were highlighted. Three participants indicated threat analysis and threat scenarios as the initial basis of training, including both cybersecurity incidents and attacks that afflict their companies, the threats that afflict other companies, as well as the common threats in their sector. Threat analysis, often based on the digital assets of the company, varies with the internal control and monitoring systems.

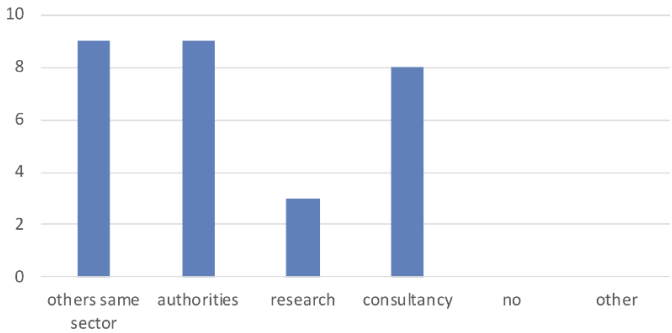

Figure 2. Number of partners for collaboration for improving the current cybersecurity initiatives

Apart from threat analysis, regulation compliance and governmental guidelines were cited as another basis of training. Companies face national or international regulations, such as European Union (EU)-wide regulations. These regulations often specify the knowledge and skills needed by cybersecurity experts, laying the basis for relevant trainings. One interviewee mentioned that the Norwegian Security Regulation Act of 2019 has a strong impact on the development and modification of internal training offerings. More specifically, the requirement of conducting risk analysis to understand acceptable risk calls for further training in risk analysis and management. Other respondents highlighted the requirements and recommendations in the ISO/IEC 27000 family of standards for the management of information risks through information security controls. In addition, two interviewees suggested that cybersecurity training in the company is developed by existing internal materials and tools for uses related to information technology, and re-purposing these instruments for cybersecurity training.

All the responding organizations cooperated with other entities to improve their cybersecurity competence (Figure 2). The most preferred entities were other organizations in the same sector (9 respondents), government authorities (9 respondents), and consultancy companies (8 respondents). Three responding organizations reported collaborating with research organizations.

5.3 Training recipients

Training was also differentiated based on the targeted recipients. Figure 3 shows the groups targeted for improvement initiatives of cybersecurity competence in the past 5 years. Nine organizations implemented such initiatives for existing general staff. The basic cybersecurity training for the general staff usually intends to raise the overall awareness in the company of cybersecurity threats and vulnerabilities, teach personnel how to reduce cybersecurity risks (e.g., the safe behaviors regarding email links or USB sticks), as well as increasing threat reporting capabilities.

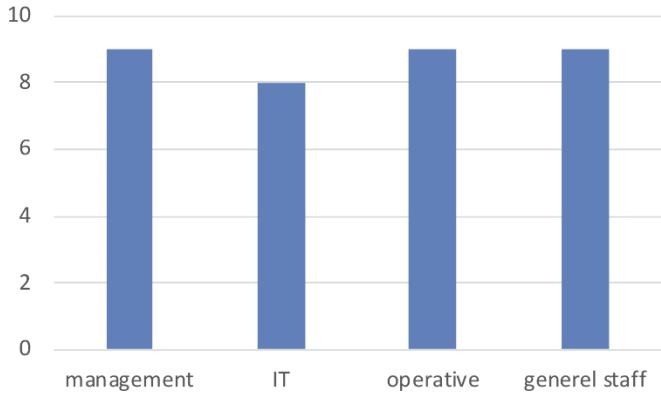

Figure 3. The number of targeted personnel groups and roles for cybersecurity initiatives over the past 5 years

Role-specific training was also offered in conjunction with general training to varying degrees. This type of training is usually designed based on the composition of the cybersecurity personnel and the teams in charge of cybersecurity infrastructure, in reference to the technical requirements of specific roles. In the past 5 years, most of the organizations provided cybersecurity training for the management, operative personnel and information technology staff (Figure 3). One interviewee stated that system administrators, application management personnel/system owners, first-line personnel, and management representatives were all recipients of training, although the training was not always differentiated by their roles. Other roles that received focused training sessions include security operations center operators, network administrators, emergency response teams, crisis management teams, and general information technology staff. In three of the interviewed organizations, part of the training offerings was also made available to any employee who had interest in developing general or specific cybersecurity competences.

All respondents reported that cybersecurity competence improvement initiatives had been realized for 2 or more of the groups in Figure 3. This response differs from the responses in Figure 1, where only 9 of the 11 respondents reported that the initiatives for developing cybersecurity competence were implemented the past 5 years. A possible reason for the difference lies in the interpretation of questions. The respondents may think about more comprehensive training initiatives, when responding to the question in Figure 1.

Still, the respondents generally agreed on the need for further improvement of cybersecurity competence, with all 11

respondents seeing this as necessary or very necessary (Figure 4). As shown in Figure 5, further improvements in cybersecurity competence were viewed as the most critical for general staff and management (8 respondents each), while 5 and 4 respondents identified information technology personnel and operative personnel as the groups in urgent need of improvements, respectively. The interviewees held that managerial roles, security operators, and cybersecurity response teams should be prioritized for specialized or focused training. Managerial roles were identified as requiring more in-depth information on threats and vulnerabilities. The provision of such information would permit timely organization of incident preparedness action plans, as well as better management of resources and organization of personnel. The personnel involved in security operation should also update their view of procedures, and have a panorama of the general threats of the company. Overall, all interviewees agreed that, basic cybersecurity training and awareness should be given to all employees, yet certain roles require more in-depth training. As such, further efforts should be taken to develop additional role-specific training offerings, which ought to provide more differentiated training to different groups of personnel.

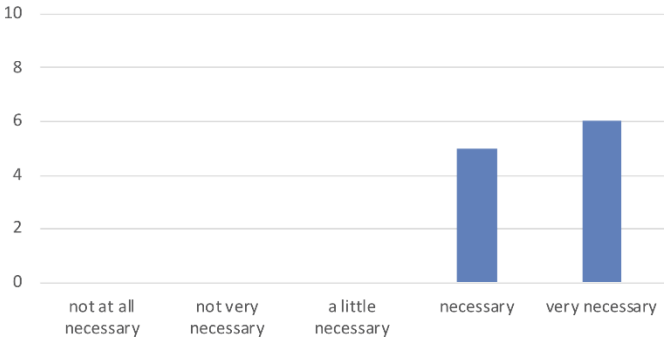

Figure 4. Number of respondents with specific views on further needs for cybersecurity competence improvements

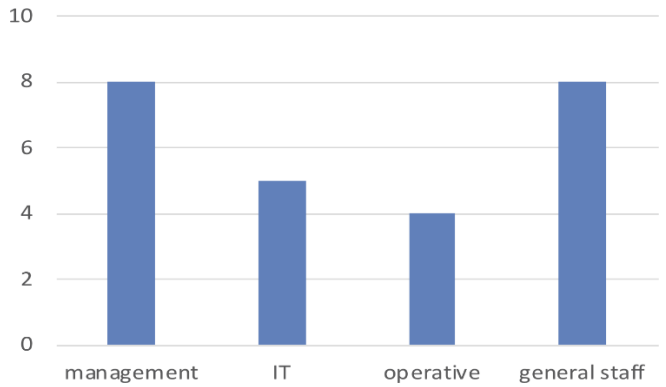

Figure 5. Roles requiring further cybersecurity competence development by each participant (multiple answers were allowed)

5.3 Training contents

The interviewees mentioned various cybersecurity topics related to the knowledge, skills and other contents being taught and developed during training. The competences and knowledge to be trained usually depend on the structural composition of the company's workforce, as well as the sector of the company. The following is a comprehensive list of all competences and skills cited in the interviews:

- Network architecture;
- Information handling (information disclosure, and information sharing and reporting);
- Cyber threats, potential cyberattacks, and system vulnerabilities;
- Procedures and preparedness plans for cyber incidents;
- Security management system (risk assessment and management, mitigation strategies, control strategies, and documentation);
- Human factors (communication, trust management, teamwork skills, and decision making);
- Surveillance;
- Crisis contingency and management;
- Incident response and management;
- Intrusion detection;
- Training of managerial skills.

The interviewees commented that some training topics were only recently integrated, and the current offerings were still in the infancy of development. In all but one of the companies, the trainees mentioned possible additions or areas needing more focus. Considerations should be given to the application of emerging technologies like artificial intelligence and blockchain in cybersecurity and big data. One respondent suggested developing training based on the holistic model of risk and incident management, providing the relevant personnel with comprehensive, modular training for the full incident management process. By analyzing the interview data, a key concern was noted: the knowledge and skills related to human factors were not fully covered. In fact, most interviewees stated that training involving communication skills, teamwork skills, and managerial skills were either lacking or underdeveloped. This was often caused by the low priority given to such activities, as well as the resource constraints that forced training to focus on the technical aspects of cybersecurity.

One interviewee proposed to train the managerial skills of the management, enabling them to make decisions when they are uncertain about the outcome, and to work under uncertainty. For the management exercises in a company, another focus is to understand the organization and proper allocation of responsibilities, e.g., the ability to handle an attack while getting the business back up and running. For the staff not working directly on cybersecurity or information technology, the training mostly focused on building cybersecurity awareness, including the information about the potential cybersecurity risks and threats, and the self-protection methods of the staff. One company implemented cybersecurity awareness initiatives, aiming to establish a healthy skepticism among the staff.

5.4 Delivery methods

According to the interviewees, multiple delivery methods were used internally to provide training. The training methods were selected based on various factors, namely, the recipients, training contents, instrumentation availability, and resource overhead. This statement was corroborated in the questionnaire responses to the specific cybersecurity competence that improves the initiatives undertaken in the past 5 years (Figure 6). All respondents reported that courses or seminars were held on cybersecurity threats, risks, or practical countermeasures 2-3 times (4 respondents) or regularly (7 respondents). The respondents disseminated information to

staff about cybersecurity threats and behaviors 2-3 times (6 respondents) or regularly (5 respondents). Cyber tests or staged attacks to evaluate cybersecurity competence (e.g., sending out fake phishing emails or penetration tests) were performed regularly by 6 organizations, 3-4 times by 3 organizations, and only once by 1 organization. Only one organization did not carry out such tests. Cybersecurity exercises were the least used initiative. Five organizations performed exercises regularly, 3 performed them once, and 3 did not conduct any cybersecurity exercise.

Figure 6. Frequency of cybersecurity awareness and training campaigns

E-learning courses were the most popular training method for both general staff and specific roles. In fact, all interviewees stated that their companies provided different forms of e-learning courses and materials. These tools were developed internally by their own companies or externally by other companies involved in the same sector. The popularity of these instruments arises from their low resource consumption, high accessibility, and ease of use. Sometimes, equivalent educational materials were offered in the company's intranet. In most cases, participation in the e-learning courses was individual and self-arranged, such that each employee can maintain a flexible training schedule, and reduced the costs and resources required for the training. The traditional form of classroom training was also offered to some groups of employees. This type of training, often provided by external entities, gained popularity among personnel. Webinars were also mentioned as a training delivery method, but seldom used. Four interviewees responded that team exercises were made available, or were part of their training program. One interviewee pointed out that training and exercises are not the same thing. Exercises intend to put competences into practice, and help to evaluate the company's response capability. Two respondents commented that the goal of an exercise is to convince the participants that they are able to do the right thing. At least part of the exercise should be at a level where staff is able to handle the situation successfully. Table-top exercises and blue-team/red-team exercises were also available. The companies that had not integrated these activities considered increasing exercise-based training. Currently, the following exercises were being considered or developed: emergency response team exercise, simulation-based exercises (operations simulation, and management simulation), and small-scale exercises (crisis management exercises, capture the flag-style exercises, and penetration test exercises). Finally, some organizations planned to stage game-based exercises.

Many forms of activities were offered to improve cybersecurity awareness: e-learning, seminars, intranet/email dissemination of information, or presentations from external speakers. Several interviewees mentioned the cybersecurity month of October as an opportunity to spread awareness. The need to find the right level and frequency of communication was also mentioned. The existing frequency (twice a year) was far from enough, as information must be repeated to keep focus on the topic. Small portions of information should be given in different channels. It is unwise to provide too much information at a time.

The questionnaire respondents reported other initiatives implemented to improve cybersecurity competence: increased focus on evaluation of information assets; courses in risk assessments and cybersecurity technologies for information technology personnel; maturity analyses; ISO 27001 certification and internal cybersecurity revision.

Although the companies did not quantify the exact impact of each measure, it is assumed that the following improvements should be achieved to enhance the company's cybersecurity:

- Compliance to policies and procedures: companies can better comply with internal policies and procedures, as well as national and international standards and policies, by incorporating the ISO 27001 certification, revising cybersecurity procedures, and attaching greater importance to information asset evaluation.
- Improved non-expert cybersecurity knowledge: companies can boost the overall preparedness against cybersecurity attacks by providing information technology personnel with courses in risk assessment and cybersecurity technologies, and improving the knowledge and competences of both cybersecurity and non-cybersecurity personnel.

Figure 7. Cybersecurity initiatives planned for the upcoming years (multiple answers were allowed)

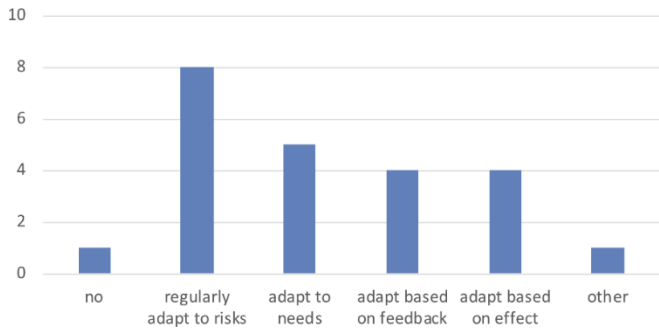

Figure 8. Basis of update and adaptation of cybersecurity initiatives (multiple answers were allowed)

Adopting proper initiatives: Among the initiatives that the organizations planned to implement soon (Figure 7), cyber tests were the most frequently mentioned (11 respondents), followed by sending out cybersecurity information (8 respondents), performing exercises (7 respondents), and holding cybersecurity courses (6 respondents). One organization planned an internal project on security culture and security competence.

The feedbacks were collected from both trainees and instructors. The purpose of feedback collection is to facilitate the identification of gaps in training contents, and the development of general suggestions for improvement. The training contents, formats, and offerings were updated sporadically according to respondents, although often tentatively scheduled yearly or at an even higher frequency. As shown in Figure 8, eight organizations regularly updated the competence-improving initiatives according to the latest risk landscape, while some made adaptations based on the needs of specific groups (5 respondents), the feedbacks from specific groups (4 respondents), or an evaluation of the effect of the initiatives (4 respondents). One organization did not make adaptations, and one organization made some adaptations, which are not systematic.

Another shortcoming of the training is the overall lack of evaluation of the trainees. Only one of the interviewees reported systematic and comprehensive evaluation of training: The training evaluation was planned before developing the training offerings, and thus influenced their development. According to the interviewee, an established framework was taken as the basis for planning and evaluation of cybersecurity exercises. Additionally, for evaluation purposes, assessing the ability of the full cybersecurity response team to resolve a threat is more valuable than evaluating the performance of each team member. This is also reflected on the evaluation methods for training exercises. In another instance, one respondent stated that the company used email-based testing to evaluate the awareness of managerial personnel of phishing attacks and social hacking risks. In addition, most interviewees stated that little to no form of evaluation was conducted at the end of the training sessions, aside feedback collection.

5.5 Personal concerns and evaluations

During the last section of the interviews, the participants were encouraged to give personal comments regarding the current standing in cybersecurity training at their companies, shortcomings in the offerings, vision for the future, and any other relevant thought. Table 6 summarizes the highlighted points raised by the interviewees. Besides topics of concern, the possible countermeasures to each topic were collected from participants, and combined with the suggestions from the literature (Table 4). In essence, these concerns reveal the under-prioritization of cybersecurity measures in these organizations, and imply the need for spending more resources on cybersecurity training and cybersecurity procedures.

Many of the respondents covered managerial roles in the development and organization of cybersecurity training offerings at their companies. Therefore, most future plans or expectations in their companies are relevant to solving the various issues noted in Table 6. The interviewees noted that their companies started to allocate more focus and resources to cybersecurity measures, rather than stick to the safety measures for physical infrastructures. Nonetheless, major flaws still presented in the internal offerings for cybersecurity training of personnel. The respondents expressed their desire of introducing more advanced and role-targeting cybersecurity training, and stated their wish for more frequent and up-to-date training courses.

Table 6. Concern topics raised by respondents and possible solutions suggested during the interviews

Topic of concern	Description	Possible countermeasures
Cybersecurity threat landscape	The cybersecurity threat landscape evolves continuously. To keep up with the latest landscape, the cybersecurity training contents should be updated frequently. This is currently lacking or not adequately implemented in most companies.	Encourage companies to invest more on content update and evaluation, and assess the current measures continuously, to ensure that procedures are up to par to the threat landscape.
Adoption of cybersecurity measures	Many of the attacks faced by companies take advantage of the poor awareness or distraction of personnel. The companies often lack adequate measures to tackle the issue.	Improve current cybersecurity awareness and training campaigns internal to the company, provide cybersecurity awareness training, and adopt various easily implementable measures to suppress the success rate of cyberattacks, e.g., authentication e-mails, and password protection.
Safety vs. cybersecurity	Most respondents commented that safety procedures are established significantly better than cybersecurity procedures. This is justified by the tradition of most CI companies: the prioritization of the safety of physical instruments over digital assets and information.	Convince the upper management to invest more resources in cybersecurity assurance, and to develop more effective cybersecurity measures. Integrate security and safety sides of the organization more deeply.
Recovery phase	Interviewees stated that procedures for the recovery phase were underdeveloped in their respective companies. This calls for improving cybersecurity training on recovery tools and procedures.	Provide comprehensive cybersecurity training, including procedures and competences about tools for recovery after a cybersecurity incident.

6. DATA ANALYSIS

To further analyze the state-of-practice of cybersecurity training in the Norwegian companies, we compared the results collected from the interviews and questionnaires to the recommendations for cybersecurity training in the literature.

As shown in Table 3, the recommendations, and best practices in the literature for developing and employing cybersecurity training offerings focus on determining training delivery methods, contents, and evaluation criteria, as well as identifying the desirable attributes of cybersecurity training offerings (scalability, accessibility, etc.).

Table 7 summarizes the recommendations in the literature for the aforementioned attributes of cybersecurity training, along with the current cybersecurity training offerings in the selected companies. It can be observed that the Norwegian

companies generally considered the best practices and other recommendations. In fact, most companies established and implemented structured strategies for cybersecurity awareness and personnel training. Following these strategies, they adopted various activities to train different roles. Despite these efforts, there are some key limitations in the current cybersecurity training offerings, and their application:

(1) Lack of role-focused training

Overall, the selected companies offered specialized training to personnel based on the specific needs associated with their roles. Yet the training needs of some roles were not satisfied. For example, the managerial roles were not sufficiently prioritized.

(2) Sub-optimal training delivery methods

A dazingly array of training offerings was cited from the participants. When it comes to training exercises, there is a lack of team-based exercises and simulation-based. These types of activities were recognized in the literature as the most effective training measures, and are highly recommended to be integrated in training programs.

Table 7. Comparison between the recommendations in the literature and the offerings of the selected companies

Attribute	Recommendations in the literature	Offerings of the selected companies
Suitability	Training should be developed based on the target audience. Specialized training should be offered to groups involved in cybersecurity activities, while basic awareness training should be given to the General staff [29].	Most companies offer specialized training for different target roles, as well as awareness activities for the general staff. Nonetheless, the key roles in the companies did not receive adequate specialized training.
Scalability and adaptability	Training offerings should be scalable to the level of knowledge and abilities of the participants, and adaptable to the sector and cybersecurity activities covered by the target audience [21].	Very limited information was collected regarding these two attributes. It was mentioned, however, that offerings were sometimes targeted to specific roles and often updated or expanded based on the feedbacks provided by participants.
Accessibility	Training should ideally be accessible both at physical locations and through remote access [13]. Possible solutions include the use of virtual labs [30], and remotely accessible testbeds and frameworks [31].	E-learning courses were one of the prevalent offerings. Additional, more interactive digital activities were suggested to be integrated to the current offerings. This was being considered by some companies.
Hands-on Experience	Training should be complemented with hands-on activities to enable trainees to deal with real-life incidents [14]. These activities instruct personnel on how to deal with real cyberattacks, and help to motivate the trainees [32]. Simulation-based exercises are recommended to boost the development of teamwork skills and communication skills [21].	Many reported the use of table-top or computer-based exercises, and some large-scale exercises. But almost no simulation or emulation-based training was currently offered. Some companies prepared plans for or expressed the interest in extending offerings to include simulation-based training. Yet the implementation of the plans is bottlenecked by resource limitations. In many companies, the offerings lacked team and communication skill development activities.
Frequency	While the frequency of training is dependent on the type of offering, continued and periodical sessions should take place. This would ensure conformity to new policies [33], as well as new technologies or vulnerabilities [34]. Similarly, updates and evaluation of training should also be conducted at scheduled frequency.	The training frequency of the companies varied with the types of activities. In some companies, the training happened periodically. Meanwhile, some companies provided only individual, non-cyclical sessions of training. The companies differed significantly in the evaluation and updates of training.
Training evaluation	The results of cybersecurity training should be evaluated by precise criteria, using pre- and post-training data, as well as other forms of evaluation [21]. Evaluation should be conducted at the end of each training cycle, to track the progress and establish possible areas of improvement.	Not all companies conducted training evaluation. In most cases, the evaluation only considered the feedbacks collected from the participants. Thus, the training may not effectively indicate the real skill acquisition or progress.

(3) Limitations in KSAs trained

The KSAs developed during the training sessions mostly involved the training of technical skills. Meanwhile, team skills, communication skills, and managerial skills were not highly prioritized. In the literature, team-based training is suggested to develop these skills. Nevertheless, factors like user behaviors, risk perception, and psychological factors [3, 35] can influence the effectiveness of these measures. Researchers are still investigating measures that account for these factors.

(4) Limited evaluation of training

Post-training evaluation was usually accomplished based on the feedbacks collected from the participants. But the collected feedbacks may not be an effective objective criterion of evaluation. In the literature, many recommended evaluating educational and training activities through personal evaluation, experimentation, and other techniques, using the key performance indicators (KPIs) [36]. The evaluation methods and KPIs should be selected during training development. Unfortunately, the research on KPIs for cybersecurity training is very limited, making it particularly challenging to select suitable indices.

(5) Infrequent training

Three of the selected companies responded that their training offerings involved cyclical training sessions. The training in other companies often contain single sessions only, or lack updates to further develop competences.

7. CONCLUSIONS

Human factors are a critical component of cybersecurity assurance. In the literature, the cybersecurity of systems hinges on the human preparedness against cybersecurity threats and attacks [37]. But the development of human preparedness is hindered by the lack of cybersecurity knowledge of personnel. National and international agencies for cybersecurity need to take urgent actions to prepare

personnel sufficiently in handling and preventing these threats [10, 23, 38], especially for companies involved in CI sectors. The CI companies play a fundamental role in the functioning of our society. Therefore, the sufficient training of their personnel should be a highly prioritized task. Unfortunately, not enough information is available in the literature to understand the state-of-practice in the training and awareness measures for CI cybersecurity, nor to identify the maturity level of these measures.

To fill the research gap, this work carries out interviews and questionnaire surveys to understand and analyze the state-of-practice in cybersecurity training and awareness offerings among selected Norwegian CI companies. The collected data were analyzed to provide details on the current practices for developing cybersecurity competence, and compared with the recommendations and best practices for cybersecurity training in the literature.

According to our analysis, the Norwegian companies all offered basic measures for cybersecurity awareness and training to their personnel, as they were increasingly aware of the benefits of cybersecurity trainings. Nonetheless, these offerings often had significant shortcomings, which were acknowledged by these companies in stating the need for further improvements in cybersecurity competence. Specifically, it was evidenced that the companies often provided specialized training only to a selected few roles or groups of personnel, although such specialized training was agreed to be advantageous for other groups within the companies. Besides, the contents and delivery methods of many offerings were limited. Communication skills, team skills, and managerial skills were often lacking or under-prioritized in the training. This is attributable to the absence or very limited availability of hands-on, team-based training in many companies, as well as the lack of resources, and the prioritization of other skills and abilities.

In the literature, simulation-based training and team exercises were regarded as the most effective ways to enhance the preparedness against real-world scenarios [21], and strongly recommended to be integrated to traditional forms of trainings. In addition, it was suggested that the collaboration between companies may help improve the less mature cybersecurity training programs. It was further noted that many companies took continued effort to improve their cybersecurity training offerings. Some companies even developed detailed action plans for introducing additional training or improving the current offerings.

The examined CI companies exhibited a common trend: cybersecurity initiatives started with small scale and limited scope, and then grew to broader and more diversified offerings throughout the organization, with the identification of further needs. However, it is a general need to further improve cybersecurity competence. One reason may be that the respondents are the persons responsible for cybersecurity in the organization. This group naturally sees the need for continuous improvements, while other roles in the organization may have different priorities and viewpoints on this matter. However, there appears to be possibilities for improvement in that cybersecurity competence initiatives were being planned and implemented. A systematic mapping of competence needs could facilitate the early identification of the cybersecurity competences needed for different roles, as well as the precise determination of the appropriate training delivery methods and evaluation of both trainees and the training programs.

Our recommendations provide useful references for plans of actions and additional measures to resolve the identified issues, as well as highlight the areas of research to be further explored to align with industry needs.

This work provides novel information and evaluation of cybersecurity awareness and training activities offered by selected Norwegian CI companies. The data were collected from 7 interviews and 11 online questionnaires. The small sample set may not exactly represent the state-of-practice of cybersecurity training in Norwegian companies. Despite that, the data still provide useful insights on commonalities in offerings and challenges faces by CI companies, which need to provide adequate cybersecurity training. The limited sample size could be justified by the fact that the study focuses on specific CI sectors, as well as the classified nature of some of the information. Nonetheless, a larger sample set would provide a more thorough overview of the state of practice.

Future work should focus on collecting additional information from more Norwegian CI companies. Getting input from other roles in the organization would uncover if there were any discrepancies in the view of cybersecurity training needs and approaches, compared to the cybersecurity practitioners. Furthermore, it would be possible to compare the state-of-practice of cybersecurity training internationally, by repeating the work and collecting data from CI companies in other countries.

REFERENCES

[1] Gritzalis, D., Theocharidou, M., Stergiopoulos, G. (2019). Critical Infrastructure Security and Resilience. Springer Cham. https://doi.org/10.1007/978-3-030-00024-0

[2] Vieane, A., Funke, G., Gutzwiller, R., Mancuso, V., Sawyer, B., Wickens, C. (2016). Addressing human factors gaps in cyber defense. Proceedings of the Human Factors and Ergonomics Society Annual Meeting. Vol. 60. 1. SAGE Publications Sage CA: Los Angeles, CA, pp. 770-773. https://doi.org/10.1177/1541931213601176

[3] Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7): e00346. https://doi.org/10.1016/j.heliyon 2017.e00346

[4] PwC 2019 PwC Cybercrime Survey url: https://publikasjoner.pwc.no/cybercrime-survey-2019/executive-summary/, accessed on 1 Sept. 2021.

[5] Venli, V. Politiet p˚a bar bakke i Norfund-saken: 100 millioner borte etter digitalt angrep. NRK. 2020. url: https://www.nrk.no/norge/politietpabarbakkeinorfundsaken_100millionerborteetterdigitaltangrep1.15015390, accessed on 1 Sep. 2021.

[6] AfternPosten 2019 Hydro har gjort fremskritt etter dataangrep. url: https://www.aftenposten.no/norge/i/OnGMXl/hydro-har-gjort-fremskritt-etter-dataangrep, accessed on 1 Sept. 2021.

[7] Hydro 2019 Cyber-attack on Hydro. url: https://www.hydro.com/en-NO/media/on-the-agenda/cyber-attack/, accessed on 1 Sept. 2021.

[8] Richardson, R., North, M.M. (2017). Ransomware: Evolution, mitigation and prevention. Faculty

Publications, 4276. https://digitalcommons.kennesaw.edu/facpubs/4276.
[9] Winnefeld Jr, J.A., Kirchhoff, C., Upton, D.M. (2015). Cybersecurity's human factor: Lessons from the Pentagon. Harvard Business Review, 93(9): 87-95.
[10] Newhouse, W., Keith, S., Scribner, B., Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. In: NIST Special Publication 800.2017 (2017), p. 181.
[11] Paulsen, C., McDuffie, E., Newhouse, W., Toth, P. (2012). NICE: Creating a cybersecurity workforce and aware public. IEEE Security & Privacy, 10(3): 76-79. https://doi.org/10.1109/MSP.2012.73
[12] McGettrick, A. (2013). Toward effective cybersecurity education. IEEE Security & Privacy, 11(6): 66-68. https://doi.org/10.1109/MSP.2013.155
[13] Pastor, V., Diaz, G., Castro, M. (2010). State-of-the-art simulation systems for information security education, training and awareness. IEEE EDUCON 2010 Conference, pp. 1907-1916. https://doi.org/10.1109/EDUCON.2010.5492435
[14] Beuran, R., Chinen, K., Tan, Y., Shinoda, Y. (2016). Towards effective cybersecurity education and training. In: Japanese Institute of Science and Technology (JAIST Repository), 1-16.
[15] Beuran, R., Pham, C., Tang, D., Chinen, K., Tan, Y., Shinoda, Y. (2017). CyTrONE: An integrated cybersecurity training framework. Proceedings of the 3rd International Conference on Information Systems Security and Privacy - ICISSP, pp. 157-166. https://doi.org/10.5220/0006206401570166
[16] Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., Baker, T. (2018). Security threats to critical infrastructure: The human factor. The Journal of Supercomputing, 74(10): 4986-5002. https://doi.org/10.1007/s11227-018-2337-2
[17] Nurse, JRC. (2021). Cybersecurity awareness. In: Jajodia, S., Samarati, P., Yung, M. (eds) Encyclopedia of Cryptography, Security and Privacy. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-27739-9_1596-1
[18] Ponsard, C., Grandclaudon, J., Bal, S. (2019). Survey and lessons learned on raising SME awareness about cybersecurity. Proceedings of the 5th International Conference on Information Systems Security and Privacy - ICISSP, Prague, Czech Republic, pp. 558-563. https://doi.org/10.5220/0007574305580563
[19] Peker, Y.K.., Ray, L., Da Silva, S., Gibson, N., Lamberson, C. (2016). Raising cybersecurity awareness among college students. Journal of The Colloquium for Information Systems Security Education, 4(1): 1-17.
[20] Bada, M., von Solms, B., Agrafiotis, I. (2019). Reviewing national cybersecurity awareness in Africa: An empirical study. https://www.thinkmind.org/index.php?view=instance&instance=CYBER+2018, 78-83. https://doi.org/10.17863/CAM.40856
[21] Chowdhury, N., Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. Computer Science Review, 40: 100361. https://doi.org/10.1016/j.cosrev.2021.100361
[22] Chowdhury, N., Gkioulos, V. (2021). Key competencies for critical infrastructure cyber-security: A systematic literature review. Information and Computer Security, 29(5): 697-723. https://doi.org/10.1108/ICS-07-2020-0121
[23] Jacob, J., Wei, W., Sha, K., Davari, S., Yang, T.A. (2018). Is the nice cybersecurity workforce framework (NCWF) effective for a workforce comprised of interdisciplinary majors?" Proceedings of the International Conference on Scientific Computing (CSC). The Steering Committee of The World Congress in Computer Science, Computer, pp. 124-130.
[24] Rahim, N.H.A., Hamid, S., Mat Kiah, M.L., Shamshirband, S., Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. Kybernetes, 44(4): 606-622. https://doi.org/10.1108/K-12-2014-0283
[25] Ricci, J., Breitinger, F., Baggili, I. (2019). Survey results on adults and cybersecurity education. Educ Inf Technol., 24: 231-249. https://doi.org/10.1007/s10639-018-9765-8
[26] Mouheb, D., Abbas, S., Merabti, M. (2019). Cybersecurity curriculum design: A survey. In: Pan, Z., Cheok, A., Müller, W., Zhang, M., El Rhalibi, A., Kifayat, K. (eds) Transactions on Edutainment XV. Lecture Notes in Computer Science(), vol 11345. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-59351-6_9
[27] Harrell, M.C., Bradley, M.A. (2009). Data collection methods. Semi-structured interviews and focus groups. Tech. rep. Rand National Defense Research Inst santa monica ca.
[28] Vaismoradi, M., Turunen, H., Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. Nursing & Health Sciences, 15(3): 398-405. https://doi.org/10.1111/nhs.12048
[29] Hoffman, L., Burley, D., Toregas, C. (2012). Holistically building the cybersecurity workforce. IEEE Security & Privacy, 10(2): 33-39. https://doi.org/10.1109/MSP.2011.181
[30] Willems, C., Meinel, C. (2012). Online assessment for hands-on cyber security training in a virtual lab. Proceedings of the 2012 IEEE Global Engineering Education Conference (EDUCON), pp. 1-10. https://doi.org/10.1109/EDUCON.2012.6201149
[31] Stites, J., Siraj, A., Brown, E.L. (2013). Smart grid security educational training with ThunderCloud: A virtual security test bed. Proceedings of the 2013 on InfoSecCD'13: Information Security Curriculum Development Conference, pp. 105-110. https://doi.org/10.1145/2528908.2528927
[32] Meso, P., Ding, Y., Xu, S. (2013). Applying protection motivation theory to information security training for college students. Journal of Information Privacy and Security, 9(1): 47-67. https://doi.org/10.1080/15536548.2013.10845672
[33] Curtis, P.D., Mehravari, N. (2015). Evaluating and improving cybersecurity capabilities of the energy critical infrastructure. 2015 IEEE International Symposium on Technologies for Homeland Security (HST), pp. 1-6. https://doi.org/10.1109/THS.2015.7225323
[34] Kang, Y.D., Chong, K.T. (2010). Development of cyber security assessment methodology for the instrumentation & control systems in nuclear power plants. Journal of the Korea Academia-Industrial Cooperation Society, 11(9): 3451-3457.

https://doi.org/10.5762/KAIS.2010.11.9.3451
[35] Evans, M., Maglaras, L.A., He, Y., Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. In: Security and Communication Networks, 9(17): 4667-4679. https://doi.org/10.1002/SEC.1657
[36] Ramsden, P. (1991). A performance indicator of teaching quality in higher education: The Course Experience Questionnaire. Studies in Higher Education, 16(2): 129-150. https://doi.org/10.1080/03075079112331382944
[37] Zimmermann, V., Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. International Journal of Human-Computer Studies, 131: 169-187. https://doi.org/10.1016/j.ijhcs.2019.05.005
[38] Shen, L. (2014). The NIST cybersecurity framework: Overview and potential impacts. Scitech Lawyer, 10(4): 16-19.

APPENDIX A

Questionnaire

Has your organization made any action to improve cybersecurity in the past 5 years? (Multiple answers possible)

- Investing in technical infrastructure
- Investing in tools to detect or handle cyber attacks
- Changing organizational structure to ensure responsibility and authority for maintaining cybersecurity
- Hiring cybersecurity expertise
- Developing the competence of existing staff
- Collaborating initiatives with other organizations
- Others:

Has your organization made any action to improve cybersecurity competence for specific groups in the past 5 years (e.g., training existing staff or hiring new staff)? (Multiple answers possible)

- Management
- Information technology personnel
- Operative personnel
- General staff
- Others:

To what extent do you think further development of cybersecurity competence is needed in your organization?

- Not at all necessary.
- Not very necessary.
- A little necessary.
- Necessary.
- Very necessary.

Do you believe there are specific groups for which improving cybersecurity competence is more critical? (Multiple answers possible)

- Management
- Information technology personnel
- Operative personnel (if relevant)
- General Staff
- Others:

To what extent has your organization performed the following measures to improve cybersecurity competence in the past 5 years? (If you have done only one type of improvement for any of the categories, please indicate the frequency of that improvement.)

Response alternatives for each category: Never, once, two-three times, and at regular interval.

- Sending out information to employees about cybersecurity threats, or how to behave with respect to cybersecurity.
- Holding courses/seminars on cybersecurity threats, risks, and practical measures.
- Staging cybersecurity tests / attacks to assess current competence (e.g., phishing, hacking, and penetration test).
- Organizing exercises to train staff (simulations at different levels, e.g., table-top, full-scale simulation of attack and response).
- Others:

Does your organization update or refine the measures for improving cybersecurity competence? (Multiple answers possible)

- No.
- Regularly adapting content to changes in the risk landscape.
- Adapting contents and forms to fit the needs of specific groups in the organization.
- Adapting contents and forms based on feedbacks from the specific groups in the organization.
- Adapting contents and forms based on evaluation of the effects of the measures.
- Others:

Does your organization collaborate with others to perform cybersecurity competence improvement in the organization? (Multiple answers possible)

- Other organizations in the same sector
- Government
- Research and academia
- Consultants
- No, we handle it ourselves.
- Others: