COMPUTER SECURITY TRAINING AND EXERCISES IN THE NUCLEAR SECTOR: INSIGHTS FROM A USER-CENTERED REQUIREMENTS GATHERING PROCESS

M.R. REISINGER
AIT Austrian Institute of Technology
Vienna, Austria
Email: michaela.reisinger@ait.ac.at

P. FRÖHLICH
AIT Austrian Institute of Technology
Vienna, Austria

P. SMITH
AIT Austrian Institute of Technology
Vienna, Austria

Abstract

Computer security is recognized as an important aspect of nuclear security: Effective measures, which include computer security education, have been integrated into nuclear security recommendations and systems. At this stage, it is crucial to understand and evaluate the current state-of-play, as perceived by (potential) recipients of education. With this understanding, informed guidance about future strategic directions can be made, to ensure that initiatives provide the most benefit to participants and the sector. The contribution of the paper is two-fold: first, results from a campaign for gathering requirements elucidate the state of computer security in the nuclear sector. Participants from thirteen countries across different roles and organization types engaged in questionnaires that aimed at identifying the state of education within their organizations, as well as impediments, perceived risks, recommendations for future interventions and key improvements for increased awareness and protection. Second, insights from the process and its results identify a set of challenges and recommendations for implementing user- and stakeholder-centered thinking in the given setting. This includes critically reflecting approaches to implement an iterative consultation process and to embed user involvement tools into the process, such as audience participation and personalized electronic questionnaires. The paper concludes with recommendations both for the design of requirements gathering processes and improved computer security training and exercises in the nuclear sector.

1. INTRODUCTION

Computer security is highlighted as an important aspect of nuclear security in Resolution 7 of the IAEA 62nd General Conference [1], which encourages states to take effective measures against cyber-attacks. Furthermore, several high-profile incidents have highlighted the need for computer security in the nuclear sector, perhaps most notably the attack associated with the Stuxnet computer worm that took place in 2010 [2].

In the nuclear context, computer security relates to the “adequate protection of any digital equipment or service from unintended access, change or destruction” [3 p. 142]. An essential aspect of protecting digital equipment and services at nuclear facilities is providing personnel with appropriate cybersecurity training. The need for training is highlighted in several IAEA guidance documents. For example, IAEA NST045 [4] states that competent authorities (regulators) should “conduct assurance activities to evaluate computer security training and skills development of competent authorities and operators” (clause 6.13) and provides further guidance about the nature of the training that should be provided (clauses 8.8 – 8.18). The importance of training is also highlighted in relevant IEC standards. For example, the IEC [5 p. 44] states that management responsibilities “include ensuring that employees and contractors (a) are properly briefed on their cybersecurity roles and responsibilities prior to being granted access to confidential information, (b) are provided with guidelines to state cybersecurity expectations of their role within the organization, (c) are motivated to fulfil the cybersecurity policies of the organization, [and] (d) achieve a level of awareness on cybersecurity relevant to their roles and responsibilities within the organization.” It also states that “all employees of the organization and, where relevant, contractors should receive appropriate awareness education, training and regular updates in organizational policies and procedures, as relevant for their job function.“ [5 p. 45].

In addition to the need for effective training programs, there is increasing awareness of the need to conduct computer security exercises to validate and evaluate capabilities within organizations and a wider nuclear security regime. Exercises for nuclear security are well-understood to be important for capacity building, as outlined in IAEA NSS 31-G [6]. Arguably, conducting exercises for computer security, specifically, is a less mature activity. Nevertheless, guidance does exist – for example, IAEA NST045 highlights the need for competent authorities to ensure that exercises evaluate a state's ability to respond to a computer security incident (clause 6.25) and further suggests that competent authorities conduct regular exercises to validate their Computer Security Plan (CSP) (clause 6.26).

As the nuclear sector's response to the need for computer security education matures, it is useful to understand and evaluate the current state-of-play, as perceived by the (potential) recipients of training. With this understanding, informed guidance about future strategic directions can be made, to ensure that initiatives provide the most benefit to participants and the sector. It is important to focus on the recipients of training and exercises because these individuals are the pracitioners and proponents for cyber security in a nuclear security regime.

This paper provides insights into user- and stakeholder-centered gathering requirements for computer security awareness and training in the nuclear energy sector. We thereby share the methodology and results of a series of recently conducted studies. These culminated in a survey of the status of computer security awareness and training from the viewpoint of experts in the field. We present the results of this study and discuss possible directions and priorities for upcoming awareness and training campaigns. We conclude by a critical reflection of the chosen approach and provide recommendations for subsequent steps of research and implementation.

2. REQUIREMENTS GATHERING CAMPAIGN

2.1. Setup

The campaign for gathering requirements for computer security training and exercises in the nuclear sector was conducted in the framework of the IAEA's CRP J02008 (Enhancing Computer Security Incident Analysis at Nuclear Facilities). It examined the current state-of-play as well as the acceptance of computer security training as perceived by (potential) recipients of training. The campaign took place in two parts: (1) a first round of questions was presented at the IAEA Technical Meeting (TM) on *Conducting Computer Security Exercises for Nuclear Security* in September 2018 to gather responses through an audience response system as well as elicit discussion. The responses and discussion contributions were used to derive first-level training recommendations and developing (2) a full questionnaire, which was then distributed to participants of the IAEA CRP J02008 project and attendees of previous IAEA training courses that are known to the authors. Additionally, the questionnaire was forwarded by these primary contacts to other potential respondents. This took place in Q1 2019.

2.2. Campaign methods: Questionnaire development

The campaign started with an audience response questionnaire at the IAEA TM on *Conducting Computer Security Exercises for Nuclear Security* in September 2018. It consisted of 13 single-choice questions (see Appendix I). The questionnaire was revised and extended based on the answers and discussions in the session. The resulting items were iteratively refined based on expert reviews. The IAEA TM session elucidated major differences between training and exercise in nuclear facilities. One of the main decisions was, therefore, to conceptually separate training and exercise. This was done by adapting questions to pertain to either separately (e.g. f - 8, 14) and to add questions to further investigate this distinction (5, 20.2). Training was defined as focusing on acquiring knowledge and building awareness, while exercise was defined as applying cybersecurity within the context of one's own work and following cybersecurity policies in practice (see also explanatory texts for respective sections in Appendix II). The adaptation also implemented responses that indicated security roles to be distinct in nuclear facilities (b - 2). Other changes included using better operationalizations (d, e – 6, 12), which allow a more accurate perspective of the state of cybersecurity education and employing open formats to allow a wider range of answers which were not available in the audience response questionnaire (e.g. 4, 11, g – 7, 13). Likewise, questions were replaced by more specific ones that made use of the greater range of operationalizations available (k – 10, 16, 23-25). One question was dropped because discussions showed that there was considerable overlap within the answer options (l). Correspondence with experts suggested risk assessments of systems to be more appropriate, which was implemented as (18) and (19). Evaluation of trainings (9) and exercises (15) were added as additional topics.

The full questionnaire (see Appendix II) consisted of 32 items in seven sections and took around 15 minutes to complete. Sections included organizational setup, the status of cybersecurity training, of cybersecurity exercises, the perceived risk of system compromise, the roles, key factors and attack vectors to be considered in the next larger training or exercise, impediments and mitigation, and geographic spread and contact opt-in.

2.3. Participants & Organizations

43 individuals completed the questionnaire partially, 31 fully. Most respondents were affiliated with more than one organization type: 19 described the type of organization they work in as an operator, 15 as a regulator, 11 as a research organization and six each as a policymaker or a technical support organization.

27 respondents chose to disclose the country in which they mainly operate, namely Argentina, Australia, Canada, Switzerland, Finland, France, Great Britain, Hungary, Mexico, Poland, Romania, Slovakia, and the USA.

3. CAMPAIGN RESULTS

In the following, we will present the current status of computer security training within the nuclear sector, as yielded by the full questionnaire. Participants from thirteen countries across different roles and organization types (e.g., operator, regulator, policymaker) engaged in the electronic questionnaire that aimed at identifying the perceived computer security risks, the current state of computer security education within their organizations, as well as impediments to education and key improvement measures for increased awareness and protection.

In 16 of 43 surveyed organizations, all staff was reported to require cybersecurity training, while most organizations target one or two specific units (e.g. IT/Network staff). Only two organizations were reported to not require cybersecurity training for any organizational units. This shows that a third of our sample engages with all employees on cybersecurity, while half of the organizations focus on specific roles. Seven of 39 respondents described their cybersecurity program as mature (structured verifiable process, dedicated resources), 14 as intermediate (structured processes, not fully supported in structure or resources), eight as basic (program consists of periodic events, but lacks rigor), seven as ad-hoc (program is random and not monitored) and three as non-existent.

Operators had programs from basic upward with a greater number of mature and intermediate programs than other organization types. Technical support organizations likewise reported training programs from basic upward. Research organizations had the most programs below basic maturity, while the responses of regulators and policymakers had a variety of maturity levels.

Ad-hoc and basic programs were described as lacking monitoring and continuous improvement as well as regularity. Respondents noted a lack of depth in both content as well as structural penetration. This was described as a strategic failing through a focus on minimum requirements and little awareness of groups and their needs. Intermediate programs were, on the other hand, described as partially incorporated in the organization, hampered by IT-structures, which are not focused on cybersecurity, with gaps in implementation, a lack of resources and daily integration. Other comments described a high quality but lack of a clear training pathway. Mature programs were implemented by dedicated task-forces (internal or external), periodically reviewed and improved. This included approaching gaps with corrective action programs, using ISO-based models or other systematic approaches. Mature programs featured a defined action plan and integration in facility management systems.

Regarding cybersecurity program focus, 54% of respondents reported a focus on training, while 20% responded to include training and exercise equally and 26% reported their organization to target neither.

38 and 34 respondents reported their training and exercise frequency (Table 1), showing a rather low intervention frequency (nearly 60% and more than 75% are receiving trainings/exercises once per year or less often).

TABLE 1. FREQUENCY OF CYBERSECURITY INTERVENTIONS.

Frequency	Training	Exercise
less often	12	14
once per year	10	12
once every 6 months	8	1
once every 3 months	5	5
more often	3	2

Training types reported included basic cybersecurity training such as presentations and video demonstrations, computer-aided learning opportunities, regional as well as international training courses, communications with internal experts and specialized training topics like portable computing and media, computer security applicable to physical security controls, or the vulnerabilities of specific technologies. Reported exercise types included responding to simulated incidents, drills, solving scenarios of hypothetical situations, evaluating fictitious investigations, walk-troughs of recovery processes, as well as round table discussions with experts.

Trainings were reported to be mostly conducted for skills development and awareness building (17 and 15 responses respectively), and less for regulatory compliance or validation of processes and procedures (9 and 5 responses respectively). Exercises were likewise conducted with a strong focus on skills re-enforcement and awareness building (15 and 11 responses), similarly also for regulatory compliance (8 responses) but slightly more for the validation of processes and procedures (10 responses).

Roughly two-thirds of respondents (62.16%, n=37) reported trainings not to be evaluated or followed-up on, while this was only the case in around half of exercises (55.88%, n=34). Looking at operators alone, slightly more than half (53.85%) and a quarter of respondents (13.08%) did not evaluate their trainings and exercises.

Training and exercise type preferences were evaluated by rankings. This showed scenario-based discussion and game-based approaches (average ranks of 4.76 and 4.19) as more interesting than more traditional training options like quizzes, information campaigns, and lectures (3.06, 3.97, and 3.97 respectively). While respondents likewise preferred scenario-based exercises (average rank of 4.03), they were followed by field exercises, tabletop exercises and game-based exercises (3.76, 3.27 and 2.88 respectively).

Safety system operation ranked as posing the highest risk if compromised among six areas, followed by *physical protection systems,* and *nuclear material accounting and control systems* (Table 2).

TABLE 2. AVERAGE RANKS OF RISK AREAS

Risk potential if compromised	Average Rank
Safety systems operation	5.15
Physical protection system	4.27
Nuclear material accounting and control systems	4.09
Corporate networks	3.33
Work management systems	2.97
Other	1.18

When gauging which roles to target with the next intervention, respondents showed that while all staff should be targeted by training more than by exercise, all specific roles (security staff, engineering/process control staff, IT/network staff, and management) should be targeted by exercises more than by trainings, especially roles with a high base knowledge like security and IT/network staff.

Industrial control system considerations, implementing the cybersecurity incident response plan and *characterizing cybersecurity incidents* were the top factors to address in the next cybersecurity intervention (Table 3). While respondents preferred a scenario-based approach for the first two, they saw field-exercises as more conductive for the third. Comments show that *industrial control system considerations* were ranked high due to their major role in nuclear safety and security, their perceived vulnerability and high risk associated with an attack (e.g. significant nuclear safety consequences). They were also noted as “most challenging to protect” due to their complexity and their technology undergoing transformation. *Implementing the cybersecurity incident response plan* was seen as a step to ensure that a plan would translate into adequate practice and timely intervention, as well as because key individuals would only be able to adhere to such a plan if they had already used it in a training environment. *Characterizing cybersecurity incidents* was noted as the basis for an adequate response and for identifying low-level indicators of an attack. The difficulty of detecting a cyber-attack was specifically outlined.

Removable media and devices was the most strongly perceived attack vector to be considered in a future intervention followed by *infected laptop*, and *lack of security culture regarding the introduction of malware* (Table 3). Removable media and mobile devices were chosen due to their ubiquity, their destructive potential and their general ability to circumvent air-gapped systems as well as their casual use by individuals (e.g. “Many people use them, often the wrong way, and it is easy to propagate malware by these methods.”). Laptops were likewise appraised as at-risk, “due to their use in public places or many networks” and as critical tools for facility management (“Laptops are used to connect to plant equipment for troubleshooting and calibration purposes. It may be the most direct way of impacting the plant critical systems, which are air-gaped.”), calling for reviewing field-equipment more rigorously. Both were also mentioned as a direct result of the third point, a lack of security culture regarding the introduction of malware, which fosters a climate without commitment or use of proper assets.

TABLE 3. AVERAGE RANKS OF KEY FACTORS AND ATTACK VECTORS TO ADDRESS WITH THE NEXT CYBERSECURITY INTERVENTION

Key factor	Average Rank [a.]
Industrial control system considerations	5.38
Implementing the cybersecurity incident response plan	5.38
Characterizing cybersecurity incidents	4.84
Nuclear security considerations	4.69
Defining response policy, roles and responsibilities	4.59
Physical protection system considerations	4.25
Cybersecurity incident communication	4.19
Information system considerations	2.69

[a.] “Other” was ranked consistently last, its average rank (1) was therefore omitted from this table.

Attack vector	Average Rank [a.]
Removable media and mobile devices	7.71
Infected laptop	7.19
Lack of a security culture regarding the introduction of malware	6.65
Subcontractor performing maintenance	5.90
Compromise of remote data links	5.71
Loss of access control and other risks posed by onsite third-party maintenance personnel	5.48
Unauthorized use of vendor backdoor accounts or hard-coded passwords	5.45
Rogue wireless connections	5.06
Loss of access control and accountability for electronic components	4.84

Ranking impediments to increasing cybersecurity awareness or skills in their organization, *lack of management focus and support* was the most salient (Table 4). Respondents based this lack of focus and support on a lack of awareness of cybersecurity importance among management, a lack of attention in the absence of “events of consequence from a nuclear cybersecurity perspective” as well as a lack of support within the current framework (e.g. “focus on safety”, “no legislation requiring cybersecurity training”).

They suggested integrating cybersecurity more firmly in the overall security scheme as well as “a culture shift towards implementing 'best practices' instead of 'minimum requirements'” to address the issue. Combatting *lack of priority or applicability* likewise included raising awareness at a senior level and tightening formal qualification requirements as well as legislation to include cybersecurity training.

TABLE 4. AVERAGE RANKS OF IMPEDIMENTS

Impediment	Average Rank
Lack of management focus and support	4.55
Lack of priority or applicability	4.13
Insufficient personnel to conduct the training	4
Insufficient funding	3.06
Lack of integration (e.g. in physical protection exercises)	2.71
Lack of motivation or incentivization	2.55

4. DISCUSSION

The results of our research show that, given a voice, respondents in the field can outline the current state of cybersecurity in the nuclear sector as well as suggest improvements to it. Responses show that classic cybersecurity issues like a lack of awareness, attention, and support on management level and within supporting frameworks also pertain to the nuclear sector.

According to the respondents, the human factor is considered in nuclear computer security programs of their organizations, but education is often regarded as limited. Only 55% of the respondents report a program that could be called adequate, which is also reflected by a third of organizations only providing few staff roles with cybersecurity education and its frequency being rarely adequate. While operators and technical support organizations were reported to have better-developed cybersecurity programs, regulators and policymakers showed a mix of lower and higher degrees of maturity. Research organizations had the least developed programs. Qualitative responses elucidated clear areas of development: Recommendations include systemic strategy development, integration in existing security structures, dedicated resources, periodic review, and corrective action programs as well as considering different target groups and their needs.

The current focus of computer security measures in many facilities is on building awareness and developing knowledge rather than application or process validation. While this reflects the emerging nature of human-centered computer security in the nuclear sector, it also points to a lack of integration. Responses furthermore showed that hands-on education is evaluated and followed-up on more than theory-driven education, and that operators evaluate both more than other groups, showing the greater maturity of their cybersecurity programs.

Education preferences suggest gamefulness to be more appropriate for knowledge-transfer and less for execution, while scenario-based interventions were found best applicable for either. Respondents indicated that all staff roles should be provided with awareness and knowledge through training sessions, while more specialized roles should rather focus on application in exercises.

Ranking key factors showed that *industrial control system considerations*, *implementing the cybersecurity incident response plan* and *characterizing cybersecurity incidents* should be addressed within the next larger training activities, employing a scenario-based approach for the first two and field-exercises for the third. Regarding attack vectors, *removable media and devices*, *infected laptop*, and *lack of security culture regarding the introduction of malware* ranked highest for consideration in a future intervention.

Participants outlined the most important impediments to increasing computer security awareness and skills in their respective organizations – namely, a lack of management focus and support, a lack of priority or applicability, and insufficient personnel to conduct the training. Qualitative responses suggest these issues to be addressed by awareness building, better framework support and developing an organizational culture that has cybersecurity in mind. Findings of this nature motivate the need for continued engagement from the IAEA to support Member States in the development of nuclear sector-specific training, as proposed in Resolution GC(62)/RES/7 [1].

5. CONCLUSION

In this paper, we provide insights into the requirements and gaps for computer security education in the nuclear sector. We derived our findings by an iterative inquiry approach that has been embedded within the framework of a multi-year international expert consultation process of the IAEA CRP program. Through an inquiry approach and its co-development with domain experts, it was possible to efficiently gain a picture of the overall current state of awareness, knowledge, and practice in the field. The iterative setup of first employing a collocated setting with audience participation as a means to refine the survey method should be regarded as a recommendable method for similar upcoming projects.

The findings on key factors, educational preferences, and computer security measures provide directions for the advancement and enforcement of cybersecurity awareness and training programs. As the next step following these first prioritizations, more specific observation and inquiry methods should be devised on-site, in order to understand the regional, cultural and technological context for the actual creation, instantiation, and implementation of the recommended measures. For this, follow-up studies with more qualitative behavioral investigations as well as user-centered requirements engineering methods may be most suitable.

ACKNOWLEDGMENTS

The research leading to these results has received funding from the IAEA as part of the CRP J02008 on Enhancing Computer Security Incident Analysis at Nuclear Facilities. We would like to thank Donald D. Dudenhoeffer, Bobby Fichman, Mitchell Hewes, Michael T. Rowland, and Christopher M. Spirito for their review of different stages of the questionnaires and their valuable insights in this process.

REFERENCES

[1] IAEA International Atomic Energy Agency, GC(62)/RES/7, 62nd General Conference, (2018). https://www-legacy.iaea.org/About/Policy/GC/GC62/Resolutions/index.html

[2] Langner, R., Stuxnet: dissecting a cyberwarfare weapon. *IEEE Secur. Priv. Mag.* **9** 3 (2011) 49–51.

[3] Berg, H.-P., Cybersecurity of critical infrastructures such as nuclear facilities. *Energetika* **63** 4 (2018) 141–145.

[4] IAEA International Atomic Energy, Computer Security for Nuclear Security Draft Implementing Guide (NST045), 2016.

[5] International electrotechnical commission, *IEC 63096:2017 - Nuclear Power Plants - Instrumentation, Control and Electrical Systems - Security Controls*. (2017).

[6] IAEA International Atomic Energy Agency, Building capacity for nuclear security. *IAEA Nucl. Secur. Ser.* **31-G** (2018).

[7] IAEA International Atomic Energy Agency, IAEA-TDL-005: Computer Security Incident Response Planning at Nuclear Facilities, Vienna, Austria (2016).

APPENDIX I: AUDIENCE RESPONSE QUESTIONNAIRE

#	Question text	Answer options	Adaptation
(a)	Organization type, see (1)	See answer options (1)	Type: multiple-choice
(b)	Organizational units attending training, see (2)	(a) security staff, (b) engineering/process control staff, (c) IT/network staff, (d) management, (e) all staff	Type: multiple-choice, (a) differentiated in cybersecurity and physical security staff
(c)	Program maturity, see (3)	See answer options (3)	
(d) (e)	When was the last time you personally took part in cybersecurity training/exercise at your workplace?	(a) 1-6 months, (b) 7-12 months, (c) 12-24 months, (d) in the past sometime, (e) never	Replaced by training (6) and exercise frequency (12)
(f)	What was the purpose of the exercise?	(a) Awareness building, (b) skills development, (c) regulatory compliance, (d) validation of process and procedures, (e) other, (f) NA (no exercise)	Type: multiple-choice, divided for training (8) and exercise (14)
(g)	What types of exercises were conducted?	See answer options (16)	Replaced by (7, 13)
(h)	Roles to target with the next training, see (20.1)	See answer options (20.1)	Changed to multiple-choice
(i)	Key factors to target, see (21)	See answer options (21)	Changed to ranking
(j)	Attack vectors to target, see (26)	See answer options (26)	Changed to ranking
(k)	What type of exercises should be conducted?	(a) tabletop, (b) field exercise, (c) scenario-based discussion, (d) game-based approaches, (e) security quizzes (to increase awareness), (f) other	Replaced by training and exercise preference (10,16), and training/exercise type to address key factors (23-25)
(l)	Which is the top cyber risk to nuclear facilities and organizations?	(a) blocking the information-flow in corporate or control networks, (b) unauthorized changes (e.g. alarm thresholds), (c) unauthorized commands to control equipment, (d) false information sent to authorized nuclear operators, (e) modification of sensitive digital asset software or configuration settings, (f) interference with safety systems operation, (g) malicious software (e.g. virus, worm, trojan horse), (h) modification of procedures or work instructions, (i) physical breaching of control systems at unstaffed remote sites (adapted from [7 p. 51 Annex IV])	Dropped, new questions formed (18, 19)
(m)	Impediments, see (28)	See answer options (28)	Changed to ranking

APPENDIX II: FULL QUESTIONNAIRE

#	Question text	Type	Answer options	Sources
[Introduction including the study context, data collection and analysis procedures as well as data protection]				
(1)	What type of organization do you work in?	multiple choice	(a) operator - physical protection systems (pps) expert, (b) operator - process control expert, (c) operator - IT/business system expert, (d) regulator, (e) policymaker, (f) technical support organization, (g) research organization, (h) contract support organization, (i) other: [text input field]	Answer options adapted from addressees of [7 p. 2]
(2)	Which organizational units are currently required to have cybersecurity training in your organization?	multiple choice	(a) cybersecurity staff, (b) physical security staff, (c) engineering/process control staff, (d) it/network staff, (e) management, (f) all staff, (g) other: [text input field]	
(3)	How would you describe your cybersecurity program?	single choice	(a) non-existent, (b) ad hoc - program is random and not monitored, (c) basic - program consists of periodic events, but lacks rigor, (d) intermediate - structured processes, but is not fully supported in structure or resources, (e) mature - structured verifiable process, dedicated resources	
(4)	Why do you consider your program *[answer from 3]*?	text input		
(5)	Does your cybersecurity program focus rather on training or on exercises?	single choice	(a) training - the program focuses on skills development and cybersecurity awareness, (b) exercise - the program focuses on cybersecurity process demonstration and following cybersecurity protocols, (c) both equally, (d) neither	
[Section introduction:] This part is about cybersecurity training: acquiring knowledge and building awareness. Training sometimes includes practical sessions, but applying cybersecurity is not their focus. While training sessions are not as closely connected to actions, they are able to give more in-depth information and provide for greater understanding of the bigger picture of cybersecurity in one's organization.				
(6)	How often do you personally take part in cybersecurity training in your workplace?	single choice	(a) more often, (b) approximately once every 3 months, (c) approximately once every 6 months, (d) once per year, (e) less often	
(7)	Which kind of training did you do? Please describe the training in your own words.	text input		
(8)	What was the main purpose of the training?	multiple choice	(a) awareness building, (b) skills development, (c) regulatory compliance, (d) validation of process and procedures, (e) other: [text input field]	
(9)	Do you evaluate trainings and follow up with their results?	single choice	yes/no	
(10)	Please rank the following training types according to your personal preference. Which training/ awareness methods provide the most value in the context of your work?	ranking	(a) scenario-based discussion, (b) game-based approaches, (c) quizzes, (d) information campaigns (e.g. poster, video), (e) lectures, (f) other *[Explanatory text]* Scenario-based discussions address realistic situations in the context of your workplace. Game-based approaches also use scenarios from other contexts, deviate more strongly from realism, or emphasize gameful experiences.	

(11)	*[If "Other" was ranked 3 or higher:]* You ranked "other" quite high - which other methods do you appreciate?	text input		
[Section introduction:] This part is about cybersecurity exercises: applying cybersecurity within the context of one's own work and following cybersecurity policies in practice. They can include knowledge transfer, but the focus of exercises lies on doing cybersecurity. While they are therefore not as closely connected to understanding and knowing about cybersecurity, they allow for testing practical implications.				
(12)	How often do you personally take part in cybersecurity exercises in your workplace?	single choice	(a) more often, (b) approximately once every 3 months, (c) approximately once every 6 months, (d) once per year, (e) less often	
(13)	Which kind of exercise did you do? Please describe the exercise in your own words.	text input		
(14)	What was the main purpose of the exercise?	multiple choice	(a) awareness building, (b) skills re-enforcement, (c) regulatory compliance, (d) validation of process and procedures, (e) other: [text input field]	
(15)	Do you evaluate exercises and prepare a corrective action plan?	single choice	yes/no	
(16)	Please rank the following exercise types according to your personal preference. Which methods would help you most to implement cybersecurity practices in the context of your work?	ranking	(a) tabletop exercise, (b) field exercise, (c) scenario-based exercise, (d) game-based exercise, (e) other *[Explanatory text see Question 10]*	
(17)	*[If "Other" was ranked 3 or higher:]* You ranked "other" quite high - which other methods do you appreciate?	text input		
(18)	Which of the following systems pose the greatest risk if compromised?	ranking	(a) safety systems operation (b) physical protection systems, (c) nuclear material accounting and control systems, (d) corporate networks, (e) work/job management systems, (f) other	Answer options adapted from [7 p. 27]
(19)	*[If "Other" was ranked 3 or higher:]* You ranked "other" quite high - which system(s) do you mean?	multiple choice	(a) emergency preparedness systems, (b) systems in a nuclear power plant that may impact the grid reliability, (c) fire detection and suppression systems, (d) other: [text input field]	
(20)	In the context of your organization, which of the following roles do you recommend for the next major cybersecurity…	2x7 matrix max. 4 choices	(1) training, (2) exercise; (a) security staff, (b) engineering/process control staff, (c) engineering/process control staff, (d) it/network staff, (e) management, (f) all staff, (g) other	
(21)	Please rank the following key factors according to how important it is to address them in the next larger training or exercise.	ranking	(a) characterizing cybersecurity incidents, (b) defining response policy, roles and responsibilities, (c) implementing the cybersecurity incident response plan, (d) cybersecurity incident communication, (e) industrial control system considerations, (f) information system considerations, (g) physical protection system considerations, (h) nuclear security considerations	Answer options adapted from key elements responding to a cyber-attack [7 p. 1]

(22)	Please describe why these three items were most relevant to you.	text input	3 fields headed by top 1-3 from (21)	
(23-25)	What type of trainings or exercises should be conducted to address *[Top 1-3 from 21]*?	multiple choice	(a) table top, (b) field exercise, (c) scenario-based approach, (d) game-based approaches, (e) security quizzes, (f) information campaigns (e.g. poster, video), (g) lectures, (h) other: [text input field]	
(26)	Please rank the following incidents/attack vectors according to how important it is to focus on them the next larger training or exercise.	ranking	(a) infected laptop, (b) removable media and mobile devices, (c) subcontractor performing maintenance, (d) rogue wireless connections, (e) loss of access control and other risks posed by onsite third-party maintenance personnel, (r) compromise of remote data links, (g) loss of access control and accountability for electronic components, (h) lack of a security culture regarding the introduction of malware, (i) unauthorized use of vendor backdoor accounts or hard-coded passwords, (j) other	Answer options adapted from potential attack vectors described in [7 p. 51 Annex IV]
(27)	Please describe why these three items were most relevant to you.	text input	3 fields headed by top 1-3 from (26)	
(28)	Please rank the following impediments according to how much they hinder increasing computer security awareness and skills in your organization.	ranking	(a) lack of management focus and support, (b) insufficient funding, (c) insufficient personnel to conduct the training, (d) lack of priority or applicability, (e) lack of motivation or incentivization, (f) lack of integration (e.g. in physical protection exercises)	
(29)	Which improvements would you see to address those issues?	text input	3 fields headed by top 1-3 from (28)	
(30)	In which country do you mainly work? *[Explanatory Text:]* This question will give us an idea of the geographical spread we were able to reach with this survey which is important for understanding and interpreting the results correctly. It will not be reported in connection with individual answers or other non-aggregated data. If you prefer not to answer this question, please proceed without selecting a country.	drop-down	*[Standard List of Countries of the World]*	
(31)	May we contact you for follow-up interviews? *[Explanatory Text:]* We will solely use your contact information for a one-time invitation in case we conduct a follow-up (in the next few months). Your contact information will not be shared with third parties and will not enter our analysis of data. It will be exported and stored separately from all other data. After export, no connection can be made between it and other answers. All data will be stored for a period of 2 years, after which it will be deleted.	single choice	Yes/No	
(32)	Please provide your e-mail address:	text input		