# Desired Cybersecurity Skills and Skills Acquisition Methods in the Organizations

**Kirsi Aaltola[1], Harri Ruoslahti[2] and Jarmo Heinonen[2]**
**[1]Finnish Institute of Public Management andUniversity of Jyväksylä, Finland**
**[2]Laurea University of Applied Sciences, Finland**
kirsi.aaltola@haus.fi
harri.ruoslahti@laurea.fi
jarmo.heinonen@laurea.fi

**Abstract**: Key personnel and their competences play important roles in continuity management and improving resilience of cybersecurity in organizations. Researchers have addressed many topics and studies in the cybersecurity domain. However, relevant cybersecurity skills and acquisition of them in expertise development, have only been partially touched. If designed systematically and properly, cybersecurity training can improve cybersecurity expertise to ensure better performance in complex cybersecurity situations. More through study on the acquisition of cybersecurity skills, and work-life needs are needed. The research three questions of this study are: How do work-life representatives see cybersecurity? How do work-life representatives see cybersecurity related skills? How do work-life representatives see methods for skills acquisition in the organizations? The work is multi-method, as it builds on both a literature review on skills acquisition in cybersecurity, and on empirical findings of a questionnaire study on cybersecurity skills desired by the work-life representatives. The findings show that cybersecurity is seen important in the organizations. The demanded skills from the employees focus especially on communication and situational awareness. There is a specific need for training with Cyber Ranges (CR) to ensure skills acquisition on cybersecurity. These results can be used to plan and design training and education for future professionals. This study aims to promote constructive discussion on skills and their acquisition in the cybersecurity domain.

**Keywords**: information technology, resilience, cybersecurity, cybersecurity skills, skills acquisition, training, cyber ranges (CRs)

## 1. Introduction

There is a need to increase cyber resilience in organizations (Aaltola & Taitto, 2019; Ruoslahti 2020), and to find solutions for the lack of skilled cybersecurity professionals in organizations (Dawson & Thomson, 2018). Recently, there have been interests to understand cybersecurity skills more comprehensively, and to build taxonomies that support the design of training of work-life needs (Furnell et al., 2017; Carlton et al., 2019). This is partly because there is a high need for professionals in the field of Information Technology (IT) (Crumpler & Lewis, 2019), and to design efficient solutions to secure digital technologies (Soni & Bhushan, 2019).

There are several research, development, and innovation (RDI) initiatives on cybersecurity on the European level, such as European Commission funded projects. This paper is based on the study conducted as part of project ECHO (European Network of Cybersecurity Centres for Innovation and Operations). Project ECHO consists of 30 partners from different sectors including health, transport, manufacturing, ICT, education, research, telecom, energy, space, healthcare, defence & civil protection. The ECHO project promotes European-wide network building, methods, and models that, within regulatory requirements, promote information sharing among network partners (Mengidis et al., 2021; Rajamäki & Katos, 2020), with a future governance model that aims to bring academia, industry, cybersecurity practitioners and end-users together (Yanakiev, 2020). This survey was conducted to provide direct input to the development Federated Cyber Ranges (FCR) concept in the ECHO project, and to serve as a potential case study to deepen understanding of skills acquisition and training in relation to the societal impacts of project ECHO.

Firstly, this paper reviews some previous literature on cybersecurity in organizations, cybersecurity skills and methods for skills acquisition. Secondly, the findings of survey responses by organizational work-life representatives on these topics are presented. Thirdly, previous findings by scholars and our findings to discuss the future directions in cybersecurity training are combined. The overall aim of the study is to improve the understanding of cybersecurity skills and their acquisition to support the work-life gaps in terms of cybersecurity expertise.

## 2. Theoretical framework

Cybersecurity combines several academic disciplines, and may therefore be seen as being a multi-disciplinary domain that joins mathematics, psychology, engineering, law and computer science (Dawson & Thomson, 2018). New technologies have radically changed the human dimension in organizations (Aaltola, 2021). Dalai et al. (2021) have emphasized increasing focus on cybersecurity work in organizations. The field has developed rapidly, which has challenged academic works in understanding what skills make a good cyber expert, and how should organizations recruit these professionals (Dawson & Thomson, 2018).

Consequences of cyberattacks may greatly vary, and new techniques to improve cyber resilience within organizations are required (Aaltola & Taitto, 2019; Ruoslahti, 2020). This literature review section of this paper focuses on viewpoints that scholars have on cybersecurity in organizations, cybersecurity skills and methods for skills acquisition. These scholarly papers mainly focus on improving cyber resilience within organizations by identifying risks and identifying different methods of cybersecurity counter measures or training.

### 2.1 Cybersecurity workforce in the organizations

Organizations must secure every critical element of their infrastructure to be well prepared to withstand threats that can compromise the security and continuity of their operations (Topham et al., 2016), also, users are often deemed a weak link due to not being educated in cyber threats concepts and not having the experience to mitigate cyber threats that may arise; e.g., social engineering and phishing are some common attacks that everyday users may encounter. Not having relevant cybersecurity training may leave them with little possibility to distinguish between a legitimate request and a cyber-attack.

Ruoslahti (2020) finds that to improve resilience and managing continuity, it is important that the network organization consider their key personnel through the possible event management stages; suggesting to 1) identify key people and develop and exercise their (cyber) skills, while in the planning phase, 2) have needed skills available during the absorb phase, and 3) broaden involved people and their skills in the recovery phase, and 4) revise the list of key people and (cyber) skills once the organization has reached the adopt phase, which would then become a new plan phase in expectation of the next unexpected cyber event.

Neal, Facteau & O'Connell (2021) offer that the growing demand for cybersecurity professionals could be solved by recruitment from "occupations with similar profiles to cybersecurity jobs include: electrical and electronics repairers, telecommunications and equipment installers and repairers, geographers, purchasing managers, personal financial advisers, sociologists and budget analysts." (p. 2/4). Modern cybersecurity specialists mainly need flexibility, as due to the available IT tools technical skills are relatively easy to master (Skorenkyy et al, 2021). Neal et al. (2021) note a shortage in cybersecurity professionals, and identify the most promising new source of future cybersecurity experts being people possessing an aptitude to acquire the new skills that make them likely to succeed in a cybersecurity career; identifying what occupations have similar work profiles and identifying the individuals who could "have the greatest potential to acquire new technical skills and succeed in cybersecurity" (p. N/A). Dawson & Thomson (2018) suggest the use of Big Five Personality traits to better understand the fit between cyber professionals and organizations.

According to Tomić et al. (2020) cybersecurity experts often begin as IT professionals, and therefore the authors suggest that tomorrow's cybersecurity experts be recruited from today's IT professionals. The study by Tomić et al., (2020) perceive among cybersecurity professionals, a lack of skills for solving different cybersecurity issues, together with poor capabilities or even unwillingness for continuously learning and skills improvement. Modern cybersecurity specialists mainly need flexibility, as due to the available IT tools technical skills are relatively easy to master (Skorenkyy et al, 2021). Nevmerzhitskaya et al. (2019) see that cybersecurity skills are needed to continuously be advanced at all levels to achieve preparedness and resilience. They suggest following "a constant learning process, to address complex demands of individual and organizational level capacity building through trainings and exercises." (Nevmerzhitskaya et al., 2019, p. 311).

### 2.2 Cybersecurity skills

Technical and engineering skills tend to become emphasized in the cybersecurity domain (Gates et al., 2014), ignoring the important social and organizational aspects needed to perform successfully in everyday work-life settings (Dawson & Thomson, 2018). Cyber professionals who work in operations maintaining security, need

significant skills and knowledge about computer systems and how to use analytical tools, such as vulnerability analysis or network scanning (Dawson & Thomson, 2018). Jajodia et al. (2010) identify a need for strong situational awareness skills, which include continuing risk assessment skills, for network professionals.

Non-technical knowledge, skills and abilities (KSA), such as problem-solving, communication and collaboration can be useful. Higher education and professional development training should integrate these non-technical KSAs into their programs that train cybersecurity professionals. (Sussman, 2021). Cyber professionals are asked to be able to communicate the technical information for the people with no technical background (Dawson & Thomson, 2018). Due to complexity of cyber domain, it has been acknowledged that cyber professionals are required to have teamwork abilities (Mathieu et al., 2000). Tomić et al. (2020) find that the most helpful IT skills for successful cybersecurity activities are use of technologies and applications, networking technologies and infrastructure, coupled with knowledge and skills of IT operations.

The skills that Neal et al. (2021) find relevant for cybersecurity professionals are critical thinking, complex problem-solving, monitoring, systems analysis, and coordination, which they would combine with technical knowledge of computers and electronics, telecommunications, customer and personal service, and administration and management. They also recommend as a suitable background experience of work activities in interacting with computers, gathering and evaluating information, updating and using relevant knowledge, making decisions and solving problems, documenting and recording information. Aaltola & Taitto (2019) raise the importance of decision-making models among cybersecurity professionals.

Dawson & Thomson (2018) discuss identifying relevant cybersecurity skills, and whether the ideal cyber workforce is required more cognitive ability than personality traits or values; the authors identify the need to determine cognitive underpinnings of the expertise that can ensure that organizations, work roles and individual skills are successfully aligned with each other.

## 2.3 Skills acquisition methods

According to Adams and Makramalla (2015) the main obstacle, which affects personnel from learning how to apply security measures and establishing cybersecurity skills, are the type of instruction they receive from cybersecurity education programs. Most programs teach security concepts with a traditional approach, where it is difficult to retain information, or to put it into practice.

Technical training is currently the prevalent form of cybersecurity education, and study programs often fail to include development cycle requirements, professional standards or regulations (Skorenkyy et al, 2021). Ghafir et al. (2018) identify challenges in implementing cybersecurity training in organizations, and promote knowing how to properly provide training that a) effectively engages non-ICT personnel to practice security awareness and to b) develop their cyber skills, and c) facilitate ICT professionals become more proficient in analysing and managing the constantly evolving cyber threats.

Aaltola and Taitto (2019) find that experiential learning principles can deepen the level of cyber learning. By supplementing theoretical knowledge with experiential learning and interactive training (e.g., games, puzzles, scenarios) for general employees could provide a more practical hands-on training that looks at real situational threats (cyber-ranges). The cognitive learning can bring the foundations to the discussions and practical solutions for acquisition of skills, but also to design of training and education for cybersecurity professionals.

Augmented reality interfaces and specialized scenarios with content that reflects the context are in use in gaming, which may be very useful in forming required competences, skills and abilities; games may be the appropriate method of implementing skills frameworks into study programs (Skorenkyy et al, 2021). Developing skills and competences, which are needed to navigate within the cyber domain are constructive processes, which use and recognize previously adapted competences of learners (Aaltola & Taitto, 2019). Simulation environments can be used to assess preparedness against cyber crises, technology failures or incidents against critical information infrastructure (Nevmerzhitskaya, Norvanto & Virag, 2019). Davis & Magrath (2013) identify skills, such as, penetration testing, hardening critical infrastructure, defending networks and responding to attacks that can be practiced in Cyber Range (CR) environments. CRs are complex IT environments where organizations can practice handling real-world cyber scenarios, and train users on the latest cyber threats. The capabilities of CRs may include simulations of real-world network environments and electronic warfare

(Priyadarshini, 2018), addressing exercises on network forensics, social engineering, reverse engineering and penetration testing, which exercises are supported by self-directed and problem-based learning (Raybourn et al., 2018). Simulations and game theories are also acknowledged methods of CRs (Wang 2010), and agent-based simulation platforms focus on simulating the effects of attacks and analyses their impacts (Grunewald et al. 2011). Practical trainings, including network simulated exercises, can be beneficial when developing relevant cyber skills (Topham et al., 2016). CRs and their features can be used as a method in cybersecurity skills acquisition, and with CRs, staff can practice their skills, identify vulnerabilities, run attack simulations and benefit CR capabilities for human improvement (Aaltola, 2021). More generally, the use of reality-virtuality technologies for learning purposes can allow more dynamic and autonomous roles in the creation of learning experiences (Ostrom et al., 2015) that may lead to higher perceptions of value (Patrício et al. 2011).

Critical discussion about the use of digital technologies in human skills acquisition often addresses challenges to transfer skills in different actual life contexts. Experts that exercise their skills in digital training platforms with the purpose to apply those skills in actual-life situations, require at least understanding of the context-specific nature of some skills, and ideally understanding of the methods that support this skills transfer from one context to another (Aaltola, 2021). Skills assessment should be built on a validated skills taxonomy, with regard to the level of the required skills, and their alignment against the job task requirements (Nevmerzhitskaya et al., 2019). Also, the use of learning outcomes in the training design ensures more thorough training needs analysis and metrics to assess learning (Aaltola & Taitto, 2019).

## 3. Research methods

To understand desired cybersecurity skills of professionals, this study collected empirical data as part of the ECHO project, and related to the development of its CR capabilities and FCR concept development. Guided by the research questions, survey questions were prepared for work-life representatives from different organizations. These survey questions were framed based on cybersecurity and cybersecurity skills, combining both, multiple-choice and open-ended questions. The multiple choice questions were framed with potential responses and an open ended “something else” alternative to choose. The survey questionnaire was sent to specified respondents selected to ensure cybersecurity expertise and experience of the respondents. The survey analysis was conducted with the sample of 43 respondents. Data validation ensured that the questionnaire was fully completed and presented the consistent data. The background data included organization related information and position in the organization. This paper presents the analysis and findings of CR cybersecurity skills study. Quantitative questions of the survey addressed mainly cybersecurity competences of the personnel in the respondents’ organizations. At first the data was analysed with factor analysis to find out groups (factors) in which loadings are connected together. The most meaningful (the highest loadings of the same factor) of the quantitative questions were analysed with correspondence analysis utilizing the Euclidean distance in two dimensional figures, where two variables and their connection to each other are presented two-dimensionally on X and Y axis. Correspondence analysis is an exploratory multivariate technique that converts a data matrix into a particular type of graphical display in which the rows and columns are depicted as points (Yelland, 2010; Greenacre & Hastie, 1987). The open ended survey responses were analysed with qualitative content analysis (Denzin & Lincoln, 1994). There were forty-three respondents (n=43) from forty European organizations. The respondents’ roles were developers, architects or engineers (n=9), managers (n=7), directors (n=5), experts, researchers or analysts (n=5), security officers (n=4), coordinators or experts (n=4) advisors or consultants (n=2), and professors (n=2). The respondents mainly represented private organizations (n = 32), while 11 of the respondents were from public organizations. By size of organization respondents represented mainly medium, over 50 employees, and large, over 250 employee, organizations, with only a few small organizations of less than five employees represented in this survey. Though, the number of responses are not sufficient to be representative of Europe, the study results are valid as a case study to provide a basis for ECHO CR development and in part to provide understanding of skills acquisition.

## 4. Results

### 4.1 Cybersecurity in the organizations

The majority of the respondents (40 of 43) described the importance of cyber security as an “important” or a “very important” thematic topic to their organization. The respondents elaborated on the importance by answering: "We have dedicated in-house competence and capability building programmes" (n=28), "We conduct regular in-house vulnerability assessments" (n=27) and "We use security as an enabler (maintaining proper cyber

hygiene and security measures positively affects business processes)" (n=24) as the most crucial reasons, while "We conduct regular vulnerability assessments by external providers" and “We have out-sourced partners for handling cyberattacks" were also mentioned as relevant reasons. However, six respondents noted that cyber security is not an important factor for their organizations. One open ended response notes that the missing parts in relation to cybersecurity are comprehensive: “The management is changing, no time for analysing the vulnerabilities, too few people, small professional staff. Too old colleagues. Not real and exact definitions, lack of knowledge of good practices.” One respondent described that they are behind the technology developments, and it is hard for the employees to keep up with the latest trends and developments. The rest of the responses focused on solutions and tools for increased data protection, and issues such as the lack of compliancy policies and standards, and challenges. For example, the age of the personnel was seen to effect organizational cybersecurity capabilities, such as preparing against vulnerabilities, and setting up Security Operation Centres (SOC) or Early Warning Systems.

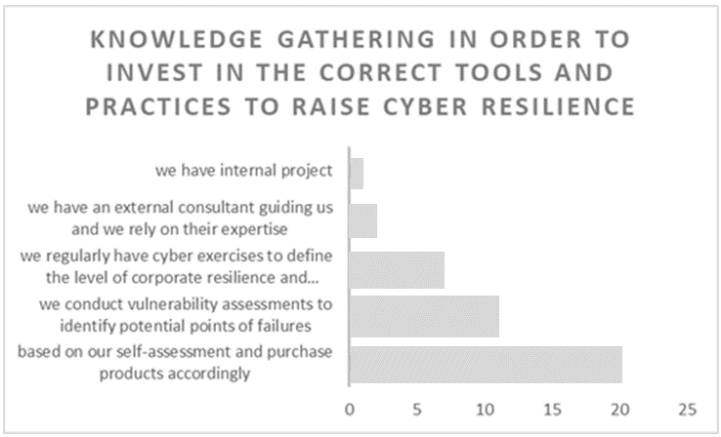


**Figure 1**: Knowledge gathering for tools to raise cyber resilience

Figure 1 shows how respondents gather the knowledge that they need to invest in the correct tools and practices that raise cyber resilience. Most respondents (n = 20) base their purchases on self-assessment, while many other conduct vulnerability assessments or conduct regular cyber exercises to determine their needs.

## 4.2 Cybersecurity skills

The respondents defined situational awareness and communication as the key cybersecurity skills that they demand from their employees. Moreover, being collaborative and approachable, but also analytical and having a hacker mind-set were seen as some key ‘skills or behavioural attributes for their employees working on cybersecurity. Based on the responses technical skills, such as understanding of the IT domain, programming, and architecture skills, are also needed, while leadership and writing skills were not seen as demanded (Figure 2).

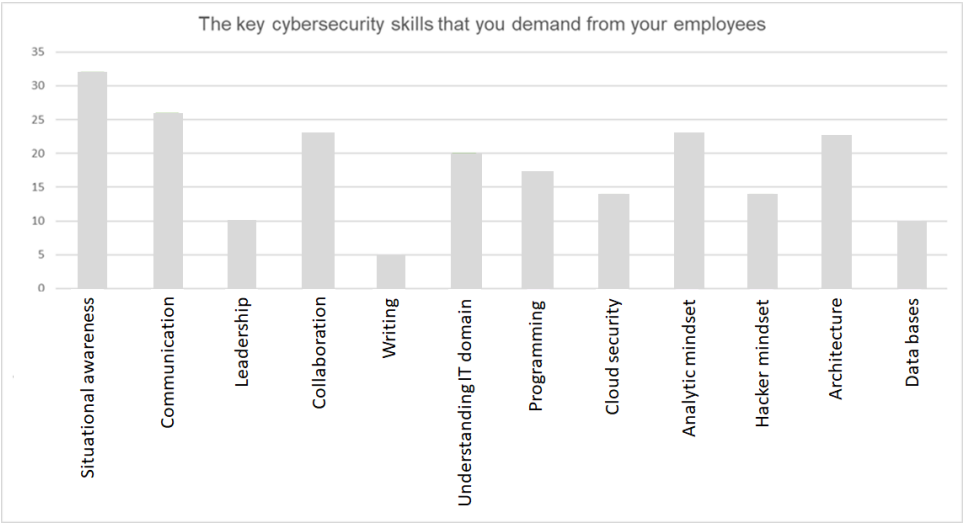


**Figure 2**: Key cybersecurity skills demanded of employees

As seen in Figure 2, Situation awareness was seen as the single most important skill for people working in cybersecurity, while in addition an appropriate array of technical skills and collaboration are needed.

### 4.3 Desired methods for skills acquisition

Seven respondents see cyber exercises as a key metric to identify correct tools and practices ("we regularly have cyber exercises to define the level of corporate resilience and identify key milestones for improvement"). The open-ended responses show seven out of twenty respondents addressing a specific training need or cyber range, while general awareness was the most needed or missing from the organization for some.

When asking about preferred usage of Cyber Range (CR), 25 of the respondents valued in-house training than external training service. The correspondence analysis conducted in the study and especially the in-house training was favoured by the organizations which had employees 25-50 or 50-250 (Figure 3).

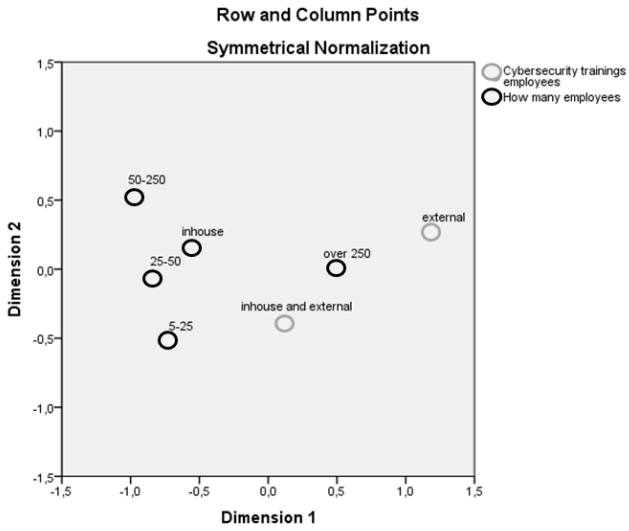


**Figure 3**: Cybersecurity trainings by type and number of employees

The technical capabilities of the CR used in the trainings focused on attack and defence simulations, learning platform and real-time monitoring. Also, traffic simulations and performance evaluation were mentioned (Figure 4).

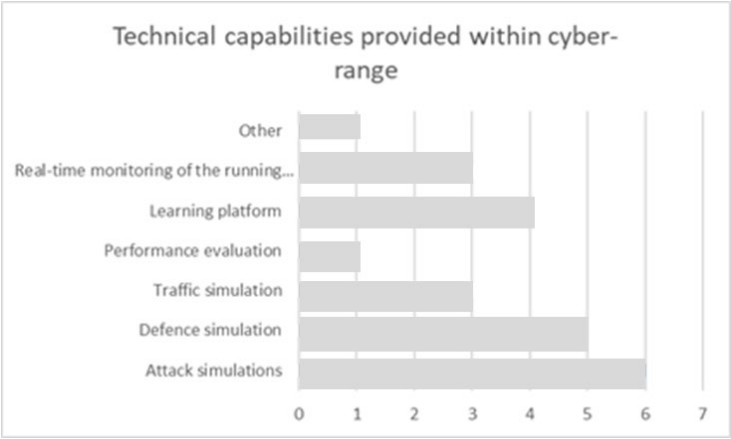


**Figure 4**: Technical capabilities of cyber ranges

On how training debriefing and performance evaluation are performed in their cyber range, three respondents noted that they have evaluation activities such as hot-wash debriefing, providing feedback that is based on the collection of data during trainings, or debriefing by company personnel. The respondents would like to further develop their sector specific capabilities (e.g., healthcare, space, transportation, energy) and provide better automation for quicker development and deployment and add automatic performance evaluation. The domain

specific approach was seen necessity and one respondent described “we always draw domain-specific expertise when create a cyber-exercise”.

## 5. Discussion

Different employees have different competences, while several vulnerabilities may occur due to the comprehensiveness of cybersecurity. Therefore, the better understanding of how important organizational representatives see cybersecurity that this study brings, supports earlier findings that cybersecurity is seen important. Different in-house capability improvements, and cybersecurity topics are seen as being complex. The respondents raise challenges, such as a lack of cybersecurity knowledge in management, lack of compliancy policies and standards, and lack of time to keep up with technology developments.

According to this study, the most desired skills for employees are situational awareness, communication, and technical skills (e.g., programming and architectural issues). In addition, having an analytical mind-set was also mentioned. The findings partly support the results of other scholars, providing in those definitions of ‘skills’ should become more un-ambiguous, and there is a need for more focus on better analysing what is meant by cybersecurity skills and by e-skills, and if these are domain-specific and their relevance to professionals in this domain.

The methods on skills acquisition were studied from the responses of both multiple choice and open-ended questions. Organizational representatives addressed the need for training, and related use of CRs. Cyber exercises are clearly a way to “define the level of corporate resilience and identify key milestones for improvement”. Many respondents value in-house training over the purchase of external training services. The technical capabilities of CRs should include attack and defence simulations, a learning platform, real-time monitoring, and capabilities to run performance evaluations. The ability to create sector-specific scenarios in CRs was seen as a positive asset.

## 6. Conclusions

The expanded use of technology has increased the research focus on cybersecurity issues that are seen being multidisciplinary. Scholars from different disciplines, who focus on studying human factors in cybersecurity raise multiple viewpoints: organisational needs, challenges and competence gaps. There seems to be a continuing need to further deepen the understanding of the specific nature of cybersecurity in organisations, with related cybersecurity skills and relevant methods of skills acquisition. Some authors have e.g., recommended solutions to narrow the current gaps in workforce within the cybersecurity field (see for example Dawson & Thomson 2018; Tomić et al., 2020; Aaltola & Taitto, 2019; Ruolahti, 2020). The findings presented in this paper help in part to describe the current situation of organisational cybersecurity, understand cybersecurity skills and different skills acquisition methods. The respondents’ (n=43) backgrounds varied, and they represented organisations with different sizes and from different European countries. Wider study will be needed to provide results that can be generalized throughout Europe, and to achieve this, the questionnaire and results of are used in the development the ECHO Societal Impact Assessment Toolkit questionnaire.

Most respondents value cybersecurity as either very important or important. They also identify several gaps in the capabilities, awareness, and employee skills within their organisations. All of these are needed to implement cybersecurity and to address related issues in everyday work life. Organizational representatives can use organisational self-assessments to gain knowledge and information on how to improve resilience, cybersecurity, mitigation and to base the purchase of new tools and solutions.

Figure 5 highlights the findings of this study. Organizations require and look for a range of skills, knowledge and attributes from their employees. In this broader context these skills can be called ‘e-skills’, as they directly relate to using ICT technology, being aware of the risks against the used ICT environment, solutions and information, and being able to address, solve or appropriately escalate possibly emerging problems and issues.

The demand for employee cybersecurity skills, as shown in the results of this study, vary from situational awareness, communication and collaboration to technical (e.g., architecture and programming) skills. In addition, attitudinal needs, such as being analytical and having a hacker mind-set were mentioned. Literature raises skills relevant to cybersecurity (e.g., Sussman, 2021; Tomić et al., 2020; Neal et al., 2021). Further study and development of organisational skills acquisition could be addressed through three relevant categories:

technical, situation awareness, and problem solving e-skills. Structuring cyber range training features, such as tailored in-house scenarios based attack simulation training, with roleplaying exercise cycles, around these three categories of e-skills may provide needed focus for impactful cybersecurity training in organizations. E.g., the ECHO E-skills and Training Toolkit will be based on these three e-skills categories.

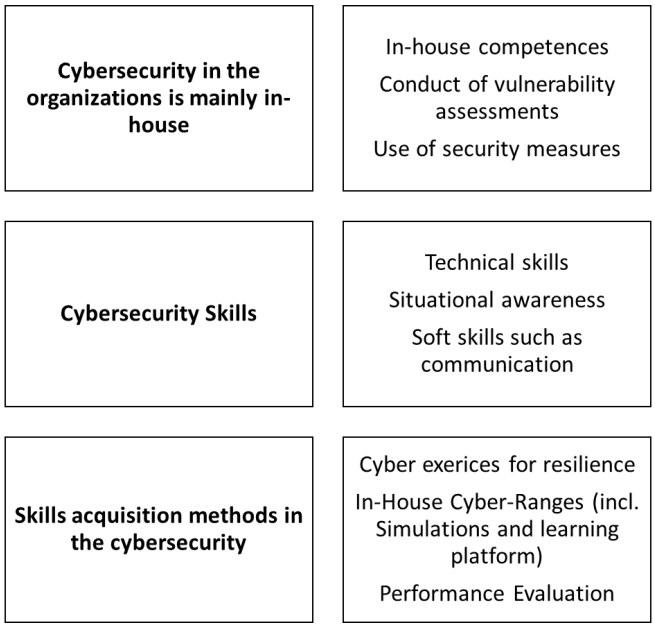


**Figure 5**: Cybersecurity in the organizations, skills and skills acquisition methods

In terms of skills acquisition, organizational representatives value cybersecurity training with CRs as a method. Relevant CRs should be uniquely designed and adapted for organisational purposes. While, modern learning environments, such as CRs are expected to promote attack and defence simulations and even real-time monitoring of the cybersecurity domain, they can be used to support skills acquisition through relevant learning platforms, and when possible, using organisational in-house capabilities. CRs cannot, however, encompass all cyber related training while, especially small and medium size organizations would prefer in-house training capabilities for experiential learning and interactive training. CRs may be too complicated to encompass all cyber related training in-house, and CR capacity can be bought from CR service providers, such as the ECHO FCR. Organisations are looking for ways to attract and develop relevant skills that take them to success. One important element in today's digitalized work and communication environments is continuity in the face of possible cyber issues and incidents. Thus, organizations are looking for better methods to identify and develop their ICT and cyber related e-skills needed to prevent, detect and address any occurring cyber incidents in a timely manner. Modern learning environments e.g., cyber ranges, provide increasing opportunities for focused skills acquisition. The model provided in Figure 5 provides a way to structure training approaches that address these three categories of e-skills in both recruitment and training. Further research and development is recommended to provide scientifically rigorous, but practical methods to identify the skills needed to successfully implement appropriate counter measures against cyber threats and incidents. Cyber ranges have so far, been mostly used to train cyber security experts. It is recommended to expand the usage of cyber ranges also for a wider range of ITC users and persons working in information intensive positions, as their careless actions may provide the needed access for a cybersecurity wrongdoer. Work-life representatives identify especially communication and situational awareness as the skills most demanded for their employees. Specified training with cyber ranges help ensure cybersecurity skills acquisition. These results can be used to plan and design practical training and education for future professionals. This study aims to promote scientific theory with its constructive discussion on cyber and e-skills and their acquisition in the cybersecurity domain.

## References

Aaltola, K. (2021). Empirical Study on Cyber Range Capabilities, Interactions and Learning. *Digital Transformation, Cyber Security and Resilience of Modern Societies*, 84, 413.

Aaltola, K., & Taitto, P. (2019). Utilising Experiential and Organizational Learning Theories to Improve Human Performance in Cyber Training. g. Information & Security: An International Journal 43, no. 2 (2019): 123-133.

Adams, M., & Makramalla, M. (2015). Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. *Technology Innovation Management Review*, 5-14.

Carlton, M., Levy, Y., & Ramim, M. (2019). Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. *Information & Computer Security*.

Crumpler, W., & Lewis, J. A. (2019). *The cybersecurity workforce gap*. Washington, DC, USA: Center for Strategic and International Studies (CSIS).

Davis, J. & Magrath, S. (2013). A Survey of Cyber Ranges and Testbeds. Cyber Electronic Warfare Division. Commonwealth of Australia 2013. October 2013.

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: going beyond technical skills for successful cyber performance. *Frontiers in psychology*, 9, 744.

Denzin N. K. & Lincoln Y. S. (1994). Handbook of Qualitative Research (Sage Publications,
Thousand Oaks, USA).

Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. *Computer Fraud & Security, 2017*(2), 5-10.

Gates, A. Q., Salamah, S., & Longpre, L. (2014). Roadmap for Graduating Students with Expertise in the Analysis and Development of Secure Cyber-Systems.

Ghafir, I., Saleem., 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, 4986-5002.

Greenacre M. and Hastie T. (1987). The Geometric Interpretation of Correspondence Analysis. Journal of the American Statistical Association, Vol. 82, No. 398 (Jun., 1987), 437-447.

Grunewald, D., Lützenberger, M, Chinnow, J. (2011). Agent-based network security simulation. In: proceedings of the 10th international conference on autonomous agents and multiagent systems. Taipei, Taiwan, 2–6 May 2011, pp.1325–1326. Richland, SC: International Foundation for Autonomous Agents and Multi-agent Systems.

Jajodia, S., & Noel, S. (2010). Topological vulnerability analysis. In *Cyber situational awareness* (pp. 139-154). Springer, Boston, MA.

Mengidis, N., Spanopoulos-Karalexidis, M., Voulgaridis, A., Merialdo, M., Raisr, I., Hanson, K., . . . Votis, K. (2021). ECHO federated cyber range: Towards next-generation scalable cyber ranges. Piscataway: The Institute of Electrical and Electronics Engineers, Inc. (IEEE). doi: http://dx.doi.org/10.1109/CSR51186.2021.9527985

Milgram, P., and Kishino, F. (1994). A taxonomy of mixed reality visual displays. IEICE Trans. Inform. Syst. E77-D, 1321–1329.

Neal, J. Facteau, J. & O'Connell, B. (2021). To find cybersecurity talent, poach from other fields. Nextgov.com (Online). Availabe: https://www.proquest.com/magazines/find-cybersecurity-talent-poach-other-fields-xa0/docview/2555709888/se-2?accountid=12003.

Nevmerzhitskaya, J., Norvanto, E., & Virag, C. (2019). High impact cybersecurity capacity building. Bucharest: "Carol I" National Defence University.

Ostrom, A., Parasuraman, A., Bowen, D., Patricio, L., Voss, A. (2015). Service research priorities in a rapidly changing context. Journal of Service Re-search, 18 (2) (2015), pp. 127-159

Patrício, L., Fisk, R. Falcão e Cunha, J. Constantine, L. (2011). Designing multi-interface service experiences: The service experience blueprint. Journal of Service Research, 10 (4) (2008), pp. 318-334

Priyadarshini, I. (2018). Features and Architecture of the Modern Cyber Range: A qualitative analysis and survey. University of Delaware. Available: http://udspace.udel.edu/handle/19716/23789 © 2018 Ishaani Priyadarshini

Raybourn E., Kunz M., Fritz D., Urias V. (2018) A Zero-Entry Cyber Range Environment for Future Learning Ecosystems. In: Koç Ç. (eds) Cyber-Physical Systems Security. Springer, Cham.

Rajamäki, J. and Katos, V., (2020). Information Sharing Models for Early Warning Systems of Cybersecurity Intelligence. Information & Security: An International Journal 46, no. 2 (2020): 198-214.

Ruoslahti, H. (2020). Business Continuity for Critical Infrastructure Operators. Annals of Disaster Risk Sciences: ADRS, 3(1), 0-0.

Ruoslahti, H., Coburn, J., Trent, A. & Tikanmäki, I. (2020). Cyber Skills Gaps – a Systematic Literature Review of Academic Literature. Submitted to a peer-reviewed journal.

Skorenkyy, Y., Kozak, R., Zagorodna, N., Kramar, O., & Baran, I. (2021). Use of augmented reality-enabled prototyping of cyber-physical systems for improving cyber-security education. Journal of Physics: Conference Series, 1840(1)

Soni, S., & Bhushan, B. (2019). Use of Machine Learning algorithms for designing efficient cyber security solutions. In *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)* (Vol. 1, pp. 1496-1501). IEEE.

Sussman, L. (2021). Exploring the value of non-technical knowledge, skills, and abilities (KSAs) to cybersecurity hiring managers. Journal of Higher Education Theory and Practice, 21(6), 99-117.

Tomić R. & Komnenić, V. (2020). Cybersecurity Talent Shortage. Annals of Disaster Risk Sciences, 3(2).

Topham, L., Kifayat, K., Younis, Y., Shi, Q., & Askwith, B. (2016). Cyber security teaching and learning laboratories: A survey. Information & Security: An International Journal, 35, 51-80.

Yanakiev, Y. (2020). A governance model of a collaborative networked organization for cybersecurity research. *Information & Security, 46*(1), 79-98.

Yelland, P. M. (2010). An introduction to correspondence analysis. The Mathematical Journal, 12(1), 86-109.

Wang, B, Cai, J, Zhang, S. (2019). A network security assessment model based on attack defense game theory. In: proceedings of the IEEE 2010 international conference on computer application and system modeling (ICCASM), Tai-yuan, China, 22–24 October 2010, pp. V3–639. Piscataway, NJ: IEEE.