Cybersecurity in Skills Development and Leadership

Ruoslahti, Harri, Laurea UAS, harri.ruoslahti@laurea.fi

Tikanmäki, I., Laurea UAS, National Defense University, ilkka.tikanmaki@laurea.fi

Abstract

Information and Communications Technology (ICT) enables organisations absorb state-of-the-art knowledge from external sources, and develop skills that promote productivity, competitiveness and organizational learning.

This study, completed as part of project ECHO efforts, aims to understand how cybersecurity is seen by PhD students specializing in it. The participants (n = 25) were asked to discuss what is cybersecurity, its elements, and users. The Typeform survey tool was used to collect, store, and analyse this data.

The results indicate that successful cybersecurity provides multi-level protection of organisational infrastructures, personal and organisational data, and financial interests of organisations. Failure to protect these may result in negative reputation, financial, ethical, and operational impacts. Human users may be the weakest link in the system, which should be seriously taken into account when deploying cybersecurity measures and administrative user privileges.

Users need to be educated in cybersecurity and be aware of threats and new developments and attacker tactics, in particular in the case of social engineering attacks. Basic technical knowledge and capabilities to detect and appropriately report attacks are needed for all levels of ICT users.

Key Words: Cybersecurity, E-skills, Technical skills, Problem-solving

1. Introduction

Cybersecurity has become more important than ever. The usage of ICT has become an increasingly important asset for organisational learning and competitiveness, as mobile and

ICT technologies advocate organizational learning, skills acquisition thus, promoting cultures of individual learning, creativity, and innovation.

People are faced with novel information management and technological paradigms that affect the cognitive learning efforts made in an organisation. ICT enables rapid search, access, and retrieval of information, lowers communication barriers, and promotes collective behaviours. But with the good, also comes the bad. Organisations need to understand what cybersecurity is and what are its elements, to be able to make the correct decisions on what devices, technologies, policies, and procedures are implemented, and how well users on all organisational levels are able to be aware and perform in case of cyber incidents.

Organisations need to identify proper levels of ICT-support and provide their people with means to acquire necessary user knowledge, skills, and abilities (KSA), referred to as 'e-skills' in this paper. This work contributes in part to the total effort of project ECHO (European Network of Cybersecurity Centres for Innovation and Operations). It consists of 30 partners from different sectors including health, transport, manufacturing, ICT, education, research, telecom, energy, space, healthcare, defence & civil protection, and the 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).

The aim of this study is to add to the overall understanding of cybersecurity, its elements, impacts and users to promote understanding of the societal impacts of cybersecurity, and to understand what cyber and e-skills are needed to effectively use ICT and cybersecurity technologies, and to be aware of cyber threats and solve cyber incidents related problems.

Research Question: What e-skills are most important in cybersecurity?

2. Cybersecurity – Learning and Skills

ICT has become more and more important in building organisational competitiveness (Mihalic & Buhalis, 2013), as ICT usage can act as a catalyst for organizational learning, generating knowledge and processing information are ways to promote productivity and competitiveness (Hortovanyi & Ferincz, 2015). ICT is a modern enabling factor with which companies, even despite limited resources, can develop the skills needed to absorb state-of-the-art knowledge from external sources (Cupiał et al., 2018). Knowledge workers can capture, store and share organizational knowledge, making their expertise available to the organisation, its network and the surrounding society (Im et al., 2013).

2.1 Cybersecurity in organisational learning

ICT enables rapidly searching, accessing and retrieving information, and this supports collaboration and communication between all stakeholders (Im et al., 2013), and ICT can offer opportunities that help enhance strategic learning (Lopez-Nicolas & Soto-Acosta, 2010).

Information systems and strategies that align with business strategies help clarify the development IT-infrastructures and prevent conflict among members of the organization (Choe, 2016). The survival of a business may depend how capable it is in implementing new IT, and how able it and its personnel are to take advantage of what opportunities new IT-solutions can offer (Hernández et al., 2010).

Leadership is needed to promote positive policies and sense of readiness to oppose any resistance to change (Cha et al., 2015), as learning is a very necessary function for organisations (Lemmetty & Collin, 2020). The use of mobile technologies has risen in the education sector (Turi et al., 2019), while ICT make storing and sharing organizational knowledge easier (Siddiqui et al., 2019). Acceptance of ICT and mobile technologies are heavily influenced by social factors, one of the main one being the perception of ease of use (Turi et al., 2019).

Self-directed learning can be integrated to the organizational ICT structures and processes in order to promote individual and continued training (Lemmetty & Collin, 2020). Competitiveness can be maintained within an innovative culture where behavioural and cognitive changes help promote organizational learning (Černe et al., 2012). ICT can play a prominent role on knowledge management (KM) in organizations, where processes, services and innovation are strongly influenced by ICT-tools to shape organizational culture (Siddiqui et al., 2019).

Usage of personal mobile and ICT technologies can be used to advocate organizational learning and promote cultures that enhance individual learning and increase innovation and creativity, and this can result in organizational productivity (Turi et al., 2019). Common learning practices (e.g., training, teamwork, continuous experimentations, sharing experiences and knowledge sources) promote success in IT-enabled organizational transformation (OT) (Cha et al., 2015).

ICT has the potential to enhance organizational learning and knowledge flows (Škerlavaj et al., 2010; Zhao & Kemp, 2013). Upgrading ICT skills with proper trainings increase people’s knowledge of how to use the various ICT tools and Knowledge Management (KM) technologies that they need to transfer and share information within and outside the organization (Conkova, 2013; Isidro-Filho et al., 2013). ICT-training upgrades ICT-skills of organization members and promotes knowledge transfers so that people can better use ICT and KM technologies (Salleh et al., 2012).

2.2 Cybersecurity skills development

To withstand threats that can compromise the security and continuity of an organisation's operations, they must secure the critical elements of their infrastructure and be well prepared (Topham et al., 2016). Many researchers see users as a weak link if not educated in cyber threats concepts and having the experience needed to mitigate the cyber threats that everyday users may encounter; e.g., in social engineering and phishing cases distinguishing a legitimate request from a cyber-attack (Topham et al., 2016). Improving resilience and managing continuity requires that organizations consider the skills and abilities of their key personnel through four event management stages 1) during the planning phase identify key people and develop their cyber skills, 2) during the absorb phase have needed skills available, 3) during the recovery phase broaden involved people and their skills, and 4) during the adopt phase revise the lists of key people and needed cyber skills (Ruoslahti, 2020).

ICT helps lower communication barriers and promote collective behaviours, enabling rapid search, access and retrieval of information, and adequate ICT support is needed to promote collaboration and communication between organizational members, and support organizational knowledge management processes (Rahman et al., 2017). As learners of today increasingly rely on ICT (Saleh & Abel, 2018), it redefines organizational professions and work processes, where people are faced with new information and technological paradigms, and cognitive learning efforts must be made (Isidro-Filho et al., 2013). Navigating the cyber domain calls for building of skills and competences, and these are constructive processes that use and recognize previously adapted competences of learners (Aaltola & Taitto, 2019).

Simulation environments can help assess preparedness against cyber and critical information infrastructure incidents and technology failures (Nevmerzhitskaya et al., 2019). Cyber Range (CR) environments, which are complex IT environments where organizations can practice handling real-world cyber scenarios and train users on the latest cyber threats, include simulations of real-world network environments and attack vectors (Priyadarshini, 2018).

3. Method

The data for this study was collected, as part of the project ECHO efforts, from the 2022 PhD Winter School held jointly by the cyber pilot projects Cyber Competence Network, Concordia, Cyber Security for Europe, SPARTA, and ECHO. The Winter School participants were asked to discuss their views on cybersecurity and pointing aspects that they see being most important to its implementation.

The discussions were held in six group workshops and the Typeform survey tool was used to collect and store the data of these small group discussions. Qualitative data analysis was conducted by placing the data into a Data Extraction Table (DET) with columns for individual themes and rows for team answers (Denzin & Lincoln, 2011). The Typeform questionnaire included an informed consent form, which the participant teams first accepted, before proceeding to document their discussions.

4. Results

The Winter School PhD students focus on the study of cybersecurity, so their views on modern cybersecurity and on important aspects to its implementation deepen our understanding of cybersecurity, its elements, and the roles of its users. This section first discusses the elements of cybersecurity and secondly the roles and skills of its users.

4.1 Elements of Cybersecurity

Cybersecurity was seen as the use of technology and legislation. Firstly, cybersecurity aims to protect and manage information. These may be the personal information of customers and employees, and all forms of organizational data. Secondly, cybersecurity protects digital infrastructures, which are computer hardware systems, networks, and software. Thirdly, cyber-physical systems (CPS) are protected by cybersecurity. Examples of CPS are Internet of Things (IoT) devices, smart cars, or smart grids. Cybersecurity can thus, be seen as a branch of computer science that studies and evaluates processes, methodologies, techniques, and applications that aim to guarantee confidentiality, integrity, and continuity of service of functions and data belonging to information systems. Cybersecurity covers all electronically and digitally connected elements or nodes, in which messages and information or signals are exchanged to each other. Interoperability between these nodes becomes ensured by technological standards and measures that must be in line with economic, legal, and ethical requirements, and agreements.

Cybersecurity measures are implemented to protect digital assets, with a focus on the actors, systems and communication channels involved to preserve confidentiality, integrity and availability of data and services. To achieve confidentiality, integrity and availability, the systems and information that need to be protected must be identified. Cybersecurity entails protecting these identified systems and information against known risks and threats, detecting new vulnerabilities and threats, and recovering from exposure to these vulnerabilities. Relevant actors, systems and channels are included in the prevention of future attacks, which is done by improving and adapting appropriate protection mechanisms and plans. The main components of security plans address the confidentiality, integrity, availability and non-repudiation of information and data. Cybersecurity includes selected sets of policies, procedures, and implementation, which together protect against unexpected events and behaviours.

The elements of cybersecurity include besides all electronic devices that participate in networks, all human individuals concerned, and fundamental security properties, regulation of data treatment processes, and technologies for enforcing these policies. Focus should be put on numerous sub-elements, such as assets, threats, risks, vulnerabilities, attack vectors and techniques, privacy and confidentiality issues, data integrity, data authentication, user authentication, user authorization, access control, non-repudiation, cryptography, and safety.

Successful cybersecurity provides multi-level protection of organisational infrastructures, of personal and organisational data, and of financial interests of commercial organisations. Failure to protect these may result in negative reputation, financial, ethical, and operational impacts. Cybersecurity is a process that consists of techniques and methods that protect both tangible and intangible assets, e.g., individuals, companies, organizations, and nations, from cyber related threats.

4.2 Roles and skills of users

Organizations may be impacted by cybersecurity, or the lack of, mainly at on an economic, reputational, legal, and social or societal level. Safety critical scenarios may create financial losses, loss of reputation, legal issues, and even direct impacts on people's safety with service interruptions, social slander, or loss of data and time. Mission critical scenarios can even cause environmental damage when processes involve the environment.

Participants in networks may have the ability to influence other network participants and nodes. Users can have multiple roles in cybersecurity. They may be attackers, defenders (white hat, data analysts, attack-response teams), victims, entry-points for attacks (social engineering), security administrators and supervisors, implementers and designers of cybersecurity policies, methodologies and technologies, or critical reviewers of issues related to cybersecurity.

Users play a key role in cybersecurity, as they must be fully aware of what risks may derive from one’s own and/or others' actions. Users must be seen as the first executors of protection policies for their own data. To protect against organisational infrastructures, and of personal and organisational data, organizations should consider security by design as a pillar element of their entire infrastructure to avoid devastating or negative economic, social, and environmental impacts. Users need to be made aware of cybersecurity threats and practices, so that they act responsibly with integrity, and avoid accidental leaks of information through e.g., social media or personal relationships. Human users may be the weakest link in the system, and this should be seriously taken into account when deploying cybersecurity measures and administrative user privileges must be restricted and managed accordingly. Users need to be educated in cybersecurity and be aware of threats, and new developments.

According to the respondents, it is important that users possess sufficient doses of critical thinking, adaptability, and trust in structured scientific processes. Besides, the ability of critical thinking, flexibility and adequate technical knowledge that is kept up to date with the latest technologies and policies. Users should be made to understand that they are integral network players, and they should acquire the skills and abilities not only to do their jobs, but also to properly operate their information systems.

Knowledge about cyber risks and threats, as well as basic security practices and policies set by organisations help users play their part in protecting the cyber assets of the organization. Everyday ICT users must also be able to use basic security software, such as antivirus software, while advanced users (e.g., cybersecurity professionals) must have advanced skills in cybersecurity, such as penetration testing, network monitoring, firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). If and if a cyber-attack were to happen, users must be informed of it, so they can react as fast as possible to minimise damages. Besides being aware of existing risks, users need basic technical knowledge, and they need to be aware of attacker tactics, in particular in the case of social engineering attacks, and they need to be capable of both detecting and reporting attacks to the responsible authorities.

Table 1 (below) provides an overview of the main results clustered in five themes. Cybersecurity are digitally connected elements. The aim of cybersecurity is to protect information, digital assets, infrastructures, and cyber-physical systems with appropriate processes, techniques, methodologies, studies, applications, technologies, and legislation. Its elements are firstly the electronic network devices and technologies for enforcing such policies, secondly regulations and policies of data treatment processes, and thirdly the individuals concerned. The main impacts on organizations are service interruptions, financial losses, and legal and reputational issues, with possibly the safety of its people.

Table 1: Overview of main results

1. Cybersecurity	– Elements that are connected digitally – Processes, techniques, methodologies, studies, applications, technology and legislation – Protect information, digital assets, infrastructures, and cyber-physical systems
2. Elements of cybersecurity	– Electronic devices in the network – Regulation of data treatment processes, and the technologies for enforcing such policies – Policies, procedures, and implementations that protect against unexpected behaviours – Individuals concerned, the fundamental security properties
3. Impacts on organizations	– Service interruptions

	– Financial losses, bad reputation, legal issues – Economic, social, and environmental – People's safety, data, and social slander
4. Roles of the user	– Participant in a network influence other network participants or nodes – Attacker, defender, victim, entry-point for attacks, security administrator, implementer, designer – First to execute protection policies for own data
5. User knowledge, skills, and abilities (KSA)	– Technical knowledge: security practices, cyber risks, threats, and security policies – Awareness of attacker tactics (especially social engineering attacks) – Critical thinking, flexibility, and adaptability

Table 1 further notes that user roles may be many: attacker, defender, victim or entry-point for attacks, security administrator, implementer, and designer. It is noteworthy that users are seen to be the first to protect their own data and be aware of that network participants influence other network nodes and participants.

5. Conclusions

The importance of cybersecurity is growing. With the growth of the usage of ICT, there are increased numbers of social engineering incidents (e.g., phishing) and attacks against individual users, or cyber-attacks against information, digital assets, infrastructures, and cyber-physical systems of organisations, and their networks. The many elements of cybersecurity, technologies, devices, data treatment processes, policies, procedures that protect against unexpected behaviours, set requirement on the knowledge, skills, and abilities (KSA) or in the case of this paper ‘e-skills’ that users need to perform in today’s digital environments.

Users need technical skills and knowledge of security practices, cyber risks, threats, and security policies, with adequate measures of awareness of attacker tactics and social engineering attacks, and critical thinking, flexibility and adaptability. These elements should be taken into account, when designing and implementing organisational learning and training programs. Modern technical environments, such as CRs, offer opportunities for constructive processes that use and recognize previously adapted competences of users in real-life scenarios.

Acknowledgement

This work was supported by the ECHO project, which has received funding from the European Union’s Horizon 2020 research and innovation programme under the grant agreement no. 830943. The European Commission funded cyber pilot projects, such as European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO), bring opportunities for researchers to conduct experiments and gather empirical data to study these aspects from different perspectives.

References

Aaltola, K., & Taitto, P. (2019). Utilising Experiential and Organizational Learning Theories to Improve Human Performance in Cyber Training. *Information & Security: An International Journal*, *43*(2), 123–133. https://doi.org/10.11610/isij.4311

Černe, M., Jaklič, M., Škerlavaj, M., Aydinlik, A. Ü., & Polat, D. D. (2012). Organizational learning culture and innovativeness in Turkish firms. *Journal of Management & Organization*, *18*(2), 193–219.

Cha, K. J., Hwang, T., & Gregor, S. (2015). An integrative model of IT-enabled organizational transformation: A multiple case study. *Management Decision*, *53*(8), 1755–1770. https://doi.org/10.1108/MD-09-2014-0550

Choe, J. (2016). The relationships among strategic performance measurement systems, IS strategic alignment, and IT infrastructure for knowledge management. *Global Business & Finance Review (GBFR)*, *21*(1), 56–72. https://doi.org/10.17549/gbfr.2016.21.1.56

Conkova, M. (2013). Analysis of Perceptions of Conventional and E-Learning Education in Corporate Training. *Journal of Competitiveness*, *5*(4), 73–97. https://doi.org/10.7441/joc.2013.04.05

Cupiał, M., Szeląg-Sikora, A., Sikora, J., Rorat, J., & Niemiec, M. (2018). Information technology tools in corporate knowledge management. *Ekonomia i Prawo. Economics and Law*, *17*(1), 5–15.

Denzin, N. K., & Lincoln, Y. S. (2011). *The SAGE Handbook of Qualitative Research* (4th ed.). Sage Publications.

Hernández, B., Jiménez, J., & Martín, M. J. (2010). Customer behavior in electronic commerce: The moderating effect of e-purchasing experience. *Journal of Business Research*, *63*(9), 964–971. https://doi.org/10.1016/j.jbusres.2009.01.019

Hortovanyi, L., & Ferincz, A. (2015). The impact of ICT on learning on-the-job. *The Learning Organization*, *22*(1), 2–13. https://doi.org/10.1108/TLO-06-2014-0032

Im, T., Porumbescu, G., & Lee, H. (2013). ICT as a Buffer to Change. *Public Performance & Management Review*, *36*(3), 436–455. https://doi.org/10.2753/PMR1530-9576360303

Isidro-Filho, A., Guimarães, T. de A., Perin, M. G., & Leung, R. C. (2013). Workplace learning strategies and professional competencies in innovation contexts in Brazilian hospitals. *BAR - Brazilian Administration Review*, *10*(2), 121–134. https://doi.org/10.1590/S1807-76922013000200002

Lemmetty, S., & Collin, K. (2020). Throwaway knowledge, useful skills or a source for wellbeing? Outlining sustainability of workplace learning situations. *International Journal of Lifelong Education*, *39*(5–6), 478–494. https://doi.org/10.1080/02601370.2020.1804004

Lopez-Nicolas, C., & Soto-Acosta, P. (2010). Analyzing ICT adoption and use effects on knowledge creation: An empirical investigation in SMEs. *International Journal of Information Management*, *30*(6), 521–528. https://doi.org/10.1016/j.ijinfomgt.2010.03.004

Mengidis, N., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2021). Cybersecurity in Next Generation Energy Grids: Challenges and Opportunities for Blockchain and AI Technologies. In T. Tagarev, K. T. Atanassov, V. Kharchenko, & J. Kacprzyk (Eds.), *Digital Transformation, Cyber Security and Resilience of Modern Societies* (pp. 299–314). Springer International Publishing. https://doi.org/10.1007/978-3-030-65722-2_18

Mihalic, T., & Buhalis, D. (2013). ICT as a new competitive advantage factor – case of small transitional hotel sector. *Economic and Business Review*, *15*(1), 33–56.

Nevmerzhitskaya, J., Norvanto, E., & Virag, C. (2019). High Impact Cybersecurity Capacity Building. *ELearning & Software for Education*, *2*, 306–312.

Priyadarshini, I. (2018). Cyber security risks in robotics. In *In Cyber security and threats: Concepts, methodologies, tools, and applications* (pp. 1235–1250). IGI Global. https://doi.org/10.4018/978-1-5225-5634-3.ch061

Rahman, S., Islam, M. Z., & Abdullah, A. D. A. (2017). Understanding factors affecting knowledge sharing: A proposed framework for Bangladesh’s business organizations. *Journal of Science and Technology Policy Management*, *8*(3), 275–298. https://doi.org/10.1108/JSTPM-02-2017-0004

Rajamäki, J., & Katos, V. (2020). Information Sharing Models for Early Warning Systems of Cybersecurity Intelligence. *Information & Security: An International Journal*, *46*(2), 198–214.

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

Saleh, M., & Abel, M.-H. (2018). System of Information Systems to support learners (a case study at the University of Technology of Compiègne). *Behaviour & Information Technology*, *37*(10–11), 1097–1110. https://doi.org/10.1080/0144929X.2018.1502808

Salleh, R., Nair, M. S., & Harun, H. (2012). Job Satisfaction, Organizational Commitment, and Turnover Intention: A Case Study on Employees of a Retail Company in Malaysia. *International Journal of Economics and Management Engineering*, *6*(12), 3429–3436.

Siddiqui, S. H., Rasheed, R., Nawaz, S., & Abbas, M. (2019). Knowledge sharing and innovation capabilities: The moderating role of organizational learning. *Pakistan Journal of Commerce and Social Sciences (PJCSS)*, *13*(2), 455–486.

Škerlavaj, M., Dimovski, V., & Desouza, K. C. (2010). Patterns and structures of intra-organizational learning networks within a knowledge-intensive organization. *Journal of Information Technology*, *25*(2), 189–204. https://doi.org/10.1057/jit.2010.3

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. https://doi.org/10.11610/isij.3503

Turi, J. A., Javed, Y., Bashir, S., Khaskhelly, F. Z., Shaikh, S., & Toheed, H. (2019). Impact of Organizational Learning Factors on Organizational Learning Effectiveness through Mobile Technology. *Quality-Access to Succsess*, *20*(171), 114–119.

Zhao, F., & Kemp, L. (2013). Exploring individual, social and organisational effects on Web 2.0-based workplace learning: A research agenda for a systematic approach. *Research in Learning Technology*, *21*. https://doi.org/10.3402/rlt.v21i0.19089