Economics and Business
ISSN 2256-0394 (online)
2025, *39*, 26–37
https://doi.org/10.7250/eb-2025-0003
Published by RTU Press

LATVIAN CYBER WORKFORCE OF TOMORROW: CLOSING THE GAP

Rūta PIRTA*, Matīss VEIGURS

Institute of Information Technology, Riga Technical University, Riga, Latvia

**Corresponding author's e-mail: ruta.pirta@rtu.lv*

Received 30.10.2024; accepted 15.01.2025

Abstract. Cybersecurity is a growing multidisciplinary job cluster in the labour market that nowadays goes beyond information technology specialists. This research paper explores the current situation and emerging gaps in cybersecurity education and employment in Latvia, specifically looking at future skills and strategies advancing human performance in the field. In the context of growing cybersecurity regulation in Europe, the workforce shortage will only increase. The research was performed by evaluating Latvian education offerings against cybersecurity competence models and skills frameworks, engaging with three focus groups of industry, governance, and education experts, and surveying organisations that require cybersecurity specialists. The study shows that organizations lack several cybersecurity roles, with the biggest emphasis on digital forensics investigators, cybersecurity architects and cybersecurity researchers. In terms of the missing competencies, organizations highlight digital forensics and cyber threat intelligence. It was concluded that cybersecurity education in Latvia is fragmented and lacks a dedicated national coordinating body. Education gaps are often filled by employers, and future education offerings should be created in close coordination with industry partners.

Keywords: *Cybersecurity, education, job roles, skills.*

JEL Classification: I21, J23, J24, O15

INTRODUCTION

Cybersecurity is one of the critical abilities for organizations to ensure resilience against disruptive events in digital and physical environments, such as cyberattacks, unauthorized access to premises, and others. In all cases, business continuity is at risk, and proper technical and managerial capabilities can help to reduce this disruption to a minimum. The global enterprise survey has considered cyber incidents the top business risk for three consecutive years (Allianz Commercial, 2024). At the same time, numerous studies and estimates point out a growing cyber workforce shortage globally. ISC2 Cyber Workforce Study 2024 estimates the global cyber workforce needed at 10.2 million with a gap of 4.8 million specialists (up from 8.1 million total with a gap of 3.4 million in 2022) (ISC2, 2024). The European Union Agency for Cybersecurity (ENISA) and the Organisation for Economic Cooperation and Development (OECD) estimate that Europe currently has a gap of at least 300 000 cyber specialists (ENISA, 2023;

OECD, 2024). Academic research confirms that widening the gap is related to several factors, where educational aspects, for example, lack of interest in the subject, lack of diversity, and overall challenges with cybersecurity education, are crucial (Blažič, 2022a).

The paper aims to investigate existing competency gaps and future education needs, considering Latvian workforce structure and industry requirements, technology development trends and related research results. The paper contributions are multi-fold. Firstly, it presents existing education provision in Latvia. Secondly, the Latvian cybersecurity workforce structure is defined. Thirdly, competence gaps and future education needs are highlighted. Finally, the paper provides recommendations about education ecosystem development, considering different stakeholder groups, such as policymakers and education institutions. The research questions (RQ) of the paper are as follows: RQ1 – What are current cybersecurity education provisions in Latvia? RQ2 – What is the structure of the cybersecurity workforce in Latvia? RQ3 – What are the current gaps in cybersecurity competencies and the future educational needs in Latvia? The research employs the design science research method (Hevner, 2007), combining desk research, experts' surveys, and experts' workshop methods.

The rest of the paper is structured as follows. Chapter 1 presents the background of the study, considering cybersecurity education standards, skills and competency frameworks. The research methodology is presented in Chapter 2. Chapter 3 provides an overview of the cybersecurity education and workforce ecosystem in Latvia. Discussion is provided in Chapter 4, and Chapter 5 concludes.

1. BACKGROUND

Cybersecurity education is mostly a decentralised topic, and there are no state-of-the-art examples of a common policy for the topic incorporation in full-cycle educational systems from primary schools up to the highest levels of university education. Systems partially executing a universal approach and moving towards systematic cybersecurity education through strategic prioritisation can be identified in the United Kingdom (Cabinet Office, 2023) and Australia (Australian Government, 2023). In the US, due to federalism, there are generally differences in education provision across the country. Thus, it is problematic to integrate cybersecurity modules due to the varying levels of knowledge in different states (Yang & Wen, 2016).

Both general awareness and specific cybersecurity knowledge of employees are associated with a reduced number of cyber incidents in organizations (Alshaikh & Adamson, 2021; Hore et al., 2024; Kweon et al., 2021). A global study on national cybersecurity strategies revealed that in the context of education development, the common tendency is aligning professional cybersecurity skills with technology security requirements and defence in a particular country/area; however, it is as important to develop a resilient and digitally mature society (AlDaajeh et al., 2022), which calls for equal efforts in providing a universal approach (some education for all) and targeted cyber professionals' training (specialized high-level programmes). There have been several attempts to map and propose universal approaches for university curricula creation and updates (Cutas et al., 2023; Dragoni et al., 2020; Payne et al., 2021; Ramezanian & Niemi, 2024).

The field in the EU is not harmonized either. It is up to sovereign states to emphasise education in their national cybersecurity strategies. However, the main institutional driver for standardization across the EU is ENISA, which has created several formal and informal initiatives in the field, such as the European Cybersecurity Challenge and Cybersecurity Higher Education Database CyberHEAD, and occasionally performs research. ENISA has identified that there are numerous cybersecurity education initiatives across Europe; however, because of the lack of experience exchange, they mostly remain as local solutions (ENISA, 2022). Another study of mostly European initiatives for kids' cybersecurity education also confirmed strong national settings, in most cases proving to be troublesome for integration into other school systems, even though a majority of them were available in English (Manganello et al., 2024). Various research projects on tertiary and adult cybersecurity education in Europe have highlighted a lack of interdisciplinarity (Cutas et al., 2023), differences between large and small countries (Dragoni et al., 2020), a lack of innovative teaching methods (e.g., gamification, simulation, situated learning), and a need for more inclusion and diversity (Rathod et al., 2023a).

Meanwhile, there are several frameworks that define cybersecurity roles, tasks and required competencies (European Union Agency for Cybersecurity, 2022), (Petersen et al., 2020). The National Institute of Standards and Technology (NIST) proposes a comprehensive Cybersecurity Workforce Framework (CWF) (Petersen et al., 2020). It compiles more than 20 suggested cybersecurity roles and maps their tasks and required competences, using a work role-based model that organizes the cybersecurity workforce into tasks, knowledge, skills, and abilities (TKSAs). The model includes such cybersecurity roles as cyber defense analyst, incident responder, vulnerability assessment analyst, security control assessor, privacy officer, and cybersecurity manager. Hovewer, the framework targets large nations and enterprises; empirically observed that Latvian cybersecurity workforce structure requires a consolidated set of roles and skills. Therefore this study follows the recently published European Cybersecurity Skills Framework (ECSF) (European Union Agency for Cybersecurity, 2022). The framework is developed by ENISA and it considers the common EU-level structure for cybersecurity roles. ECSF is more targeted to medium-sized enterprises, and it includes nine different cybersecurity roles and their competences: chief information security officer (CISO); cyber incident responder; cyber legal, policy and compliance officer; cyber threat intelligence specialist; cybersecurity architect; cybersecurity auditor; cybersecurity educator; cybersecurity implementer; cybersecurity researcher; cybersecurity risk manager; digital forensics investigator; and penetration tester. Both frameworks highlight a different set of technical and non-technical competences, required to perform the daily duties of different cybersecurity roles.

Interdisciplinarity in terms of cybersecurity competences is also highlighted in several related research studies (Blažič, 2022b; de Casanove & Sèdes, 2021; ISC2, 2023; Pirta-Dreimane et al., 2022). The required skillset of cybersecurity professionals of today and tomorrow combines 3 main pillars – technical fundamentals of computer science, social and human aspects and competences required for the protection of emerging technologies. Technical fundamentals include ground skills in cybersecurity, such as understanding basic computer architectures, data, cryptography, networking, secure coding principles, and operating systems (Blažič, 2022b). Social and human aspects of cybersecurity cover the requirement for systemic thinkers, team players, a love for continued learning, strong communication ability, a sense of civic duty, and a blend of technical and social skills (Dawson & Thomson, 2018; Blažič, 2022b). While main required skills to safely use and protect emerging technologies (ISC2, 2023; Rathod et al., 2023a, 2023b; Blažič, 2022b): cloud computing security, artificial intelligence/machine learning and Zero Trust implementation, big data, blockchain, IoT, cyber-physical systems, network software, mobile device and software engineering technologies. Technological topics should incorporate soft-skill competencies, such as critical thinking in cybersecurity risk management and collaboration and communication in cybersecurity incident management, among others.

2. METHODS AND PROCEDURES

The study employs the design science research method (Hevner, 2007), which aims to solve practical problems by providing domain-specific solutions. The method empowers multiple studies and research methods in the process of three repeatable cycles. The relevance cycle uses the environmental context and provides research requirements to improve the knowledge base and solve the research problem. The design cycle includes artefact development and evaluation. The rigor cycle supports the research with prior knowledge and ensures the solution is innovative. The overview of the research methodology is presented in Fig. 1.

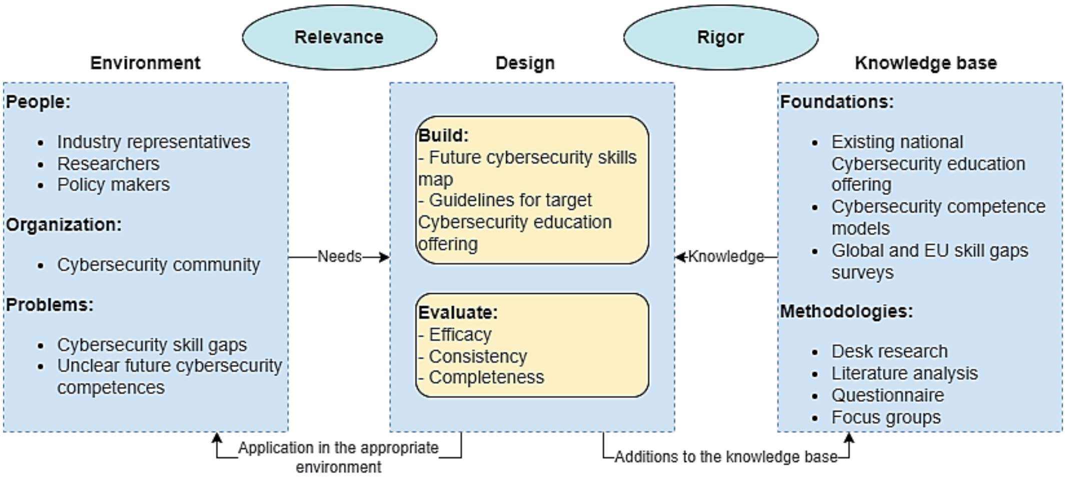


Fig. 1. Research methodology.

This research identifies future cybersecurity skill needs and provides tailored recommendations for academic, policy, and industry stakeholders regarding cybersecurity education provision in Latvia. Using a design science approach, the study integrated desk research, literature review, focus groups, and survey data analysis. An initial desk review assessed Latvia's current cybersecurity educational offering at different levels, along with workforce requirements. The investigation included various sources, such as the Latvian open data portal, State Employment Agency of Latvia registers and Latvian vacancies portals. Future cybersecurity skills and potential gaps were mapped and refined based on input from 45 local cybersecurity experts via a national survey and a workshop convened by the European Cybersecurity Competence Centre (ECCC) National Coordination Center of 35 cybersecurity specialists across public, industry, and educational sectors to explore educational needs across various education levels in March–April 2024. Using Lean UX Canvas, participants collaboratively defined problems, stakeholders, opportunities, and success metrics, forming key insights for Latvia's cybersecurity education roadmap and informing future policy decisions.

3. RESEARCH RESULTS

The research results are presented in the next sections, considering two main dimensions – the cybersecurity education ecosystem in Latvia (Section 3.1) and the cybersecurity workforce ecosystem in Latvia (Section 3.2).

3.1. Cybersecurity Education in Latvia

Cybersecurity education in Latvia is provided at all levels (topics incorporated in general basic education, specific vocational and higher education programmes up to the second cycle (Master's) level), except PhD level, where there is no specific programme or research subsector dedicated to cybersecurity. There are various non-formal initiatives and programmes provided for children and adults, mostly driven by market demand.

3.1.1. Formal Cybersecurity Education

Cybersecurity topics in general basic education are incorporated into various subjects due to the competencies-based education model adopted in 2020/2021. Topics broadly refer to three types of education outcomes – *awareness* (cybersecurity knowledge), *hygiene* (everyday skills and actions for digital safety), and *response* (skills and competencies necessary for dealing with cybersecurity incidents; a basis for a cybersecurity career track) (MK not. Nr. 416, 2019; MK not. Nr. 747, 2018). Primary education does touch upon some response topics; however, generally, it does not concentrate on skills necessary for the cybersecurity career track. Secondary education might provide deeper knowledge only if certain school provides the highest level courses in Programming and Design & Technology. According to the National Centre of Education, such courses are available only in approximately 1/3 of Latvian schools, which are mostly concentrated in larger cities (Riga, Liepaja, Ventspils, Rezekne, Cesis) (Skola, 2030, 2020) and host more students than average, which creates uneven entry positions into tertiary cybersecurity education after graduation for students coming from rural areas and small educational institutions as confirmed by the results of programming exams (regions active + overall results depending on the size of the municipality) (VISC, 2024).

Vocational cybersecurity education is provided only in one institution – “Cybersecurity Technician” at Saldus Vocational School. Some other programmes have an introduction to cyber topics, for example, “Junior Military Instructor” at O. Kalpaks Professional Secondary School and programmes “Programming Technician” and “Computer Systems Technician” across the country. In August 2024, a professional standard for “Cybersecurity Technician” (EQF 4) was approved in Latvia which may facilitate the replication of similar programmes to the one provided by Saldus Vocational School in other educational institutions.

Higher education addresses cybersecurity competences by incorporating cybersecurity-related courses into study programs and by establishing specialized study programs in cybersecurity. Cybersecurity higher education programs are provided by four educational institutions in Latvia: Riga Technical University, BA School of Business and Finance, Vidzeme University of Applied Sciences, and College of Law. College of Law provides a short cycle study program, “Security and Personal Data Protection”. The study program aims to ensure an opportunity to obtain the profession of security specialist and educate for professional activities in the field of security and personal data protection (College of Law, 2021). Vidzeme University of Applied Sciences provides a bachelor-level study programme, “Information Technology” (with specialization in Cybersecurity), and a professional master-level study programme, “Cybersecurity Engineering”. The bachelor-level study programme aims to promote the development of the IT industry by educating new specialists, thus promoting the creation of new and innovative products and services. The master-level study programme aims to provide the necessary competencies for a cyber security specialist who is responsible for strengthening information systems as well as preventing cyber-attacks and security incidents, carrying out risk analysis and offering security measures to mitigate threats in their workplace or an external client. BA School of Business and Finance provides a master-level study programme “Cybersecurity Management”. The study programme aims to provide persons with an opportunity to acquire the profession of Information Security Manager and to prepare them for professional activities to ensure information security and cybersecurity management in the organization. Riga Technical University provides a master-level study programme, “Cybersecurity Engineering”, to provide a set of theoretical knowledge and practical skills for students to achieve competencies corresponding to a master's degree in cybersecurity engineering. In the academic master's studies, the student acquires the necessary knowledge, skills and competence for comprehensive and effective action in the field of cybersecurity engineering in the chosen economic sector. In addition to dedicated cybersecurity study programmes, cybersecurity courses are also integrated into various other academic programmes. These courses are primarily found within computer science programmes, but some are also offered in social sciences, law, and civil defense programmmes. The focus of these courses is predominantly on technical skills, with less attention to human factors. Most cybersecurity-related courses are included at the master’s level.

3.1.2. Non-formal Cybersecurity Education

Children and teenagers get involved in non-formal education mostly through personal interest and less through guided efforts as there are almost no top-down initiatives for that (interest groups set by educational institutions, specific policies, etc.); mostly guided efforts are seen in general computer science topics, especially programming and robotics (Izglītības un zinātnes ministrija, 2021). There are annual *Capture the Flag* competitions for enthusiasts, such as *Kiberplēsis* (private sector initiative since 2022) and National Cybersecurity Challenge (Ministry of Defence and their public sector partners' initiative since 2024). A non-formal extracurricular military education programme of the Youth Guard is accessible in all regions of the country and offers a little insight into cybersecurity topics (up to 5 % of the content throughout 8 years) (Jaunsardzes centrs, 2021).

Non-formal cybersecurity education for adults is usually facilitated through self-learning or specific upskilling or reskilling courses. There are a few public sector efforts to make self-learning more accessible through financed access to MOOC platforms (e.g., *Coursera*), for example, in projects run by the State Education Development Agency and State Employment Agency. There are several training companies in the market which offer generic and specific cybersecurity courses, including training for internationally recognised certificates (e.g., CISM, CEH, CISSP, CFR-410, and CompTIA Security+/Pentest+/CASP/CySa+). Several companies in the private sector offer bootcamps (e.g., *Accenture*, *TietoEvry*, *TestDevLab*, *MageBit*), but none specifically focus on cybersecurity career track. Such social initiatives like *Riga Tech Girls* and *Women4Cyber* promote gender balance and inclusion in the field while also providing training and mentorship.

3.2. Cybersecurity Workforce in Latvia

The existing cybersecurity workforce structure in Latvia can be observed in professional standards and employment data (Subsection 3.2.1). Meanwhile the survey of the enterprises discovers a wider set of existing and missing cybersecurity roles and competences (Subsection 3.2.2).

3.2.1. Professional Standards and Employment Data

Latvian professional standards provide requirements for professional education. In April 2024, four cybersecurity-related professions were defined: information security engineer, information security manager, information systems security specialist, and security specialist. Meanwhile, employment and vacancies data analysis show that enterprises also have other cybersecurity roles. Overall, over 12 distinct roles in cybersecurity are observed, including information system security manager, information technology security analyst/engineer, data privacy analyst/data protection officer, and security risk management specialist. Overall, observed roles in employment data sources match with ENISA recommendations, showing a diverse set of required cybersecurity experts and competences. In the meantime, several ENISA roles are compiled into one cybersecurity role, showing the need for a wider set of competences, which is a common situation in smaller nations.

3.2.2. Results of the Organizations' Survey

Surveyed organizations in Latvia most commonly reported roles of chief information security officer (CISO) (62 %), cyber incident responder (22 %), cybersecurity risk manager (18 %), and penetration tester (18 %). The situation reflects typical vacancies and the EU-wide tendency of organizations in small countries to combine cyber job roles in "umbrella" positions such as CISO. The least represented roles in surveyed organizations were digital forensics investigator (2 %), cybersecurity architect (4 %), and cybersecurity researcher (4 %). 31 % of surveyed organizations reported no cybersecurity specialists, while all acknowledged the need for such personnel.

The educational background of employed cybersecurity specialists in surveyed organizations is mostly related to the field. Over 70 % of organizations employ specialists with relevant vocational or higher education. However, in 27 % of organizations, the most common profile of a cybersecurity specialist is a person without a relevant educational background but with the necessary knowledge and skills. This is a sign of employers' flexibility, involvement in the development of their workforce, and individuals' self-learning capabilities.

Survey participants also identified current competency gaps in their cyber workforce. 49 % of organizations reported a need for digital forensics capabilities. Almost as crucial needs are cyber threat intelligence skills and cybersecurity architecture and specific development skills (both 47 %). Future competency needs evaluation revealed that the most desirable is knowledge of basic computer science, systems thinking, critical thinking, and desire for continuous learning (4.5 points out of 5).

3.2.3. Results of the Experts' Workshop

Experts' workshop was designed to engage them in discussions regarding cybersecurity education in general, vocational/higher, and non-formal/lifelong levels, and its effects on the workforce, as well as to propose solutions for tackling identified problems. Out of 35 participants, 10 represented public institutions engaged in cybersecurity education shaping, 12 were associated with the cybersecurity industry, and 13 were experts from educational institutions, including students.

Experts stressed that general education institutions lack overall security awareness and cyber hygiene knowledge specifically, both among employees and students. Often there is no appropriate ICT policy and technical configuration of devices in place. Not all IT teachers in schools are equipped to provide support in cybersecurity matters. Experts suggested strengthening non-formal education initiatives and incorporating cybersecurity topics in curricula of other subjects, including strengthening general skills such as critical thinking. Teachers need to be trained on appropriate delivery of the topic; in case of the introduction of new devices in schools, teachers have to receive informational and practical support on the safe use of the equipment.

Vocational and higher education, according to experts, lacks cyber hygiene topics in non-IT-related programmes. It is partly related to an overall shortage of educators, especially outside of the IT domain. In Latvia, there are only Master's programmes specifically dedicated to cybersecurity; the lack of such programmes at the Bachelor's and Doctorate levels creates a gap in the workforce. Educational institutions are slow to react to local industry demands, while prospective employees are hired early by global service centres located in Latvia and provide tailored training. Experts suggested integrating cybersecurity topics in all programmes (similar to civil security courses) and recognizing cybersecurity as a separate field in education classification, which would allow the creation of more specific programmes, including a Doctorate degree. Programmes need to correspond to the most demanded cybersecurity certifications. Further development also requires the consolidation of learning materials in one repository and the introduction of research grants specifically for cybersecurity topics.

Non-formal and lifelong learning was described as fragmented: there are various educators with various qualities; information regarding these opportunities is also scattered. There is no coordinating body for these initiatives; thus, they often lack formal recognition in the job market. In expert's opinion, these education initatives need to be coordinated, regulated, and communicated by some government body, possibly using already existing lifelong learning platforms.

4. DISCUSSION

This study investigated the existing cybersecurity education ecosystem in Latvia, along with competency gaps and future education needs. Organizations lack the following main cybersecurity roles: digital forensics investigator, cybersecurity architect and cybersecurity researcher. Organizations highlight digital forensics and cyber threat intelligence as key missing competences today. Consequently, digital forensics capabilities have been identified as the most crucial area in need of improvement. This can be addressed by providing specialized educational programs in multiple formats, as currently, these competences are less represented in the educational offerings. Organizations highlight several future competency needs, including basic computer science knowledge, critical thinking, systems thinking, and a desire for continuous learning. These competencies should be considered when revising current education programs and designing new ones. Experts' workshop revealed that the introduction of cybersecurity topics to overall society, increased non-formal activities, support for teachers, and integration of cybersecurity into a wider array of educational programs, along with the establishment of doctoral programs and a research grant system in cybersecurity, could facilitate closing the cyber workforce gap.

CONCLUSIONS

It was concluded that there is a significant shortage of cybersecurity professionals and skills, with the gap continuing to expand. Cybersecurity education in Latvia is fragmented and lacks a dedicated national coordinating body. General education includes some cybersecurity topics, but deeper knowledge is limited to select schools, and overall cyber hygiene in schools is insufficient. Non-formal education for both children and adults is available but fragmented, with a need for better coordination and quality assurance. Higher education institutions do offer integrated topics or specific cybersecurity programmes; however, it is not enough for current industry needs. Further research is needed to assess the precise gap in the cyber workforce and more tailored industry needs, especially after the introduction of the National Cybersecurity Law, which sets strict cybersecurity requirements for thousands of Latvian organizations across various industries.

ACKNOWLEDGEMENT

This study was supported by the EU Digital Europe programme within the project "National Coordination Centre – Latvia" (NCC-LV) under Grant Agreement No. 101127985.

REFERENCES

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Raymond Choo, K.-K. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*, 102754. https://doi.org/10.1016/j.cose.2022.102754

Allianz Commercial. (2024). Allianz Risk Barometer: Identifying the major business risks for 2024.

Alshaikh, M., & Adamson, B. (2021). From awareness to influence: toward a model for improving employees' security behaviour. *Personal and Ubiquitous Computing*, *25*(5), 829–841. https://doi.org/10.1007/s00779-021-01551-2

Australian Government. (2023). 2023–2030 Australian Cyber Security Strategy.

Blažič, B. J. (2022a). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? *Education and Information Technologies*, *27*(3), 3011–3036. https://doi.org/10.1007/s10639-021-10704-y

Blažič, B. J. (2022b). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? *Education and Information Technologies*, *27*(3), 3011–3036. https://doi.org/10.1007/s10639-021-10704-y

Cabinet Office of United Kingdom. (2023). National Cyber Strategy 2022: Annual Progress Report 2022– 2023. Cabinet Office of United Kingdom.

College of Law. (2021). Self-evaluation report of the study field "Management, Administration and Management of Real Property" 2021/2022. https://jk.lv/en/2023/08/14/2700-educational-institutions-and-study-programs-recommended-by-employers/

Cutas, F., Chatzopoulous, A., Athanatos, M., & Antonakaki, D. (2023). CONCORDIA Governance Model for a European Education Ecosystem for Cybersecurity.

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. In *Frontiers in Psychology* (Vol. 9, Issue JUN). https://doi.org/10.3389/fpsyg.2018.00744

de Casanove, Nicolas Leleu, Florence Sèdes. Applying PDCA to Security, Education, Training and Awareness Programs. 16th IFIP WG 11.12 International Symposium on Human Aspects of Information Security and Assurance (HAISA 2022), IFIP TC 11 Working Group 12: Human Aspects of Information Security and Assurance, Jul. 2022, Mytilenne, Lesvos, Greece, pp. 39–48.

Dragoni, A. Lluch Lafuente, A. Schlichtkrull, and L. Zhao, "D6.2 education and training review,"Cybersec4europe, 2020. https://cybersec4europe.eu/wp-content/uploads/2020/02/D6.2-Education-and-Training-Review-V1.2-Submtted.pdf

ENISA (2022). Cybersecurity Education Initiatives in the EU Member States.

ENISA. (2023, September 21). Cybersecurity Skills Conference: Strengthening human capital in the EU. https://Www.Enisa.Europa.Eu/News/Cybersecurity-Skills-Conference-Strengthening-Human-Capital-in-the-Eu.

European Union Agency for Cybersecurity, E. (2022). European cybersecurity skills framework. https://Www.Enisa.Europa.Eu/Publications/European-Cybersecurity-Skills-Framework-Role-Profiles.

Hevner, A. R. (2007). A Three Cycle View of Design Science Research. *Scandinavian Journal of Information Systems*, *19*(2), 4. http://community.mis.temple.edu/seminars/files/2009/10/Hevner-SJIS.pdf

Hore, K., Hoi Tan, M., Kehoe, A., Beegan, A., Mason, S., Al Mane, N., Hughes, D., Kelly, C., Wells, J., & Magner, C. (2024). Cybersecurity and critical care staff: A mixed methods study. *International Journal of Medical Informatics*, *185*, 105412. https://doi.org/10.1016/j.ijmedinf.2024.105412

ISC2. (2023). ISC2_Cybersecurity_Workforce_Study_2023. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e

ISC2. (2024, September 11). Employers Must Act as Cybersecurity Workforce Growth Stalls and Skills Gaps Widen. https://Www.Isc2.Org/Insights/2024/09/Employers-Must-Act-Cybersecurity-Workforce-Growth-Stalls-as-Skills-Gaps-Widen

Izglītības un zinātnes ministrija. (2021). Pētījums par izglītības piedāvājuma pārklājumu un izglītojamo iesaisti STEM jomā.

Jaunsardzes centrs. (2021). *Jaunsargu interešu izglītības programma.* Jaunsardzes centrs.

Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence. *Information Systems Frontiers*, *23*, 361–373. https://doi.org/10.1007/s10796-019-09977-z

Manganello, F., Earp, J., Fante, C., Bassi, G., Fabbri, S., Matteucci, I., Vaccarelli, A., Olesen, N., de Vibraye, A., Callaghan, P., & Gentile, M. (2024). Shaping the foundation of the SuperCyberKids Learning Framework: a comprehensive analysis of cybersecurity education initiatives. *Frontiers in Education*, *9*. https://doi.org/10.3389/feduc.2024.1375853

Ministru Kabineta Noteikumi Nr. 416 (2019). Noteikumi Par Valsts Vispārējās Vidējās Izglītības Standartu Un Vispārējās Vidējās Izglītības Programmu Paraugiem.

Ministru Kabineta Noteikumi Nr. 747 (2018). Noteikumi Par Valsts Pamatizglītības Standartu Un Pamatizglītības Programmu Paraugiem.

OECD. (2024). Building a Skilled Cyber Security Workforce in Europe. Insights from France, Germany and Poland. https://doi.org/10.1787/3673cd60-en

Payne, B. K., He, W., Wang, C., Wittkower, D. E., & Wu, H. (2021). Cybersecurity, Technology, and Society: Developing an Interdisciplinary, Open, General Education Cybersecurity Course. *Journal of Information Systems Education*, *32*(2), 134–149. https://doi.org/10.21428/cb6ab371.8113760b

Petersen, R., Santos, D., Smith, M., Wetzel, K., & Witte, G. (2020). *Workforce Framework for Cybersecurity (NICE Framework)*. NIST Special Publication 800-181, Revision 1, 3.

Pirta-Dreimane, R., Brilingaitė, A., Majore, G., Knox, B. J., Lapin, K., Parish, K., Sütterlin, S., & Lugo, R. G. (2022). Application of intervention mapping in cybersecurity education design. *Frontiers in Education*, *7*. https://doi.org/10.3389/feduc.2022.998335

Ramezanian, S., & Niemi, V. (2024). Cybersecurity Education in Universities: A Comprehensive Guide to Curriculum Development. *IEEE Access*, *12*, 61741–61766. https://doi.org/10.1109/ACCESS.2024.3392970

Rathod, P., Ofem, P., Polemi, N., Hynninen, T., Lugo, R. G., Alcaraz, C., Kioskli, K., & Rannenberg, K. (2023a). D2.1 Cybersecurity Practical Skills Gaps in Europe: Market Demand and Analyse.

Rathod, P., Ofem, P., Polemi, N., Hynninen, T., Lugo, R. G., Alcaraz, C., Kioskli, K., & Rannenberg, K. (2023b). D2.1 Cybersecurity Practical Skills Gaps in Europe: Market Demand and Analyse. Lead Author Contributing Participants.

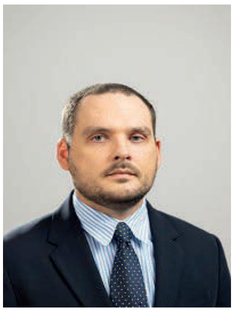
Skola2030. (2020). Skolu piedāvājums vidējā izglītībā. https://skola2030.lv/admin/filemanager/files/2/VSK%20PK_20.04.2020%20_final_ppt.pdf.

VISC. (2024, October 9). Valsts pārbaudes darbi 2023./2024. m.g. Statistika. Https://Www.Visc.Gov.Lv/Lv/Valsts-Parbaudes-Darbi-20232024-Mg-Statistika.

Yang, S. C., & Wen, B. (2016). Toward a cybersecurity curriculum model for undergraduate business schools: A survey of AACSB-accredited institutions in the United States. *Journal of Education for Business*, *92*(1), 1–8. https://doi.org/10.1080/08832323.2016.1261790

AUTHORS' SHORT BIOGRAPHY

Rūta Pirta has over 15 years of experience in the IT field, specializing in information security, enterprise architecture, and digital transformation. She is a Senior Researcher, Assistant Professor, and Director of the "Information Technology Project Management" programme at Riga Technical University. Rūta leads multiple cybersecurity and information security courses at the graduate and continuing education levels. Her research focuses on human-centered cybersecurity education, the use of serious games for cybersecurity training, and IT security risk management in service and partner ecosystems.
E-mail: ruta.pirta@rtu.lv
ORCID iD: https://orcid.org/0000-0001-8568-0276



Matīss VEIGURS is a System Analyst at the National Cybersecurity Centre's Unit of European Union Cybersecurity Affairs (Ministry of Defence of the Republic of Latvia). He received a Social Sciences Master's Degree in Political Science (2014) from the University of Latvia and an Engineering Sciences Master's Degree in Digital Humanities (2023) from the Riga Technical University (RTU). He is currently pursuing a Professional Master's Degree in information technology with an IT Project Manager's professional qualification from RTU.
E-mail: matiss.veigurs@edu.rtu.lv
ORCID iD: https://orcid.org/0009-0000-6061-6526