ADDRESSING CYBERSECURITY CHALLENGES IN LATVIAN SMES: LEGAL, HUMAN, AND ECONOMIC DIMENSIONS OF DIGITAL TRANSFORMATION

***Dace Kadile[1], Laura Kadile[2], Baiba Rivza[1]**
[1]Latvia University of Life Sciences and Technologies, Latvia
[2]Riga Graduate School of Law, Latvia
*Corresponding author's e-mail: Dace.Kadile@gmail.com

Abstract
In today's business environment small and medium-sized enterprises (SMEs) are constantly adapting to the era of digital transformation. The rapid integration of technology has catalysed digital transformation and engendered unprecedented challenges. The aim of this research is to ascertain the most pertinent cybersecurity risks for SMEs in the times of digital transformation. The study focus is on the cybersecurity standards, requirements and provision of support mechanisms established by the European Union and Latvian national legal frameworks. The empirical research analyses the human factor in cybersecurity for SMEs. The study revealed human, organisational, technological and security risks as significant cybersecurity risks for SMEs. The findings of the empirical study conducted reveal that continuous self-development, characterised by the acquisition of new skills and competencies, is conducive to the human resource perspective of digital transformation. Three fundamental objectives were identified to support the goals of cybersecurity and digital transformation. These are the availability of funding, public-private cooperation and education for enterprises. The study concludes that the development of robust legal and economic policies is fundamental to ensure the protection of SMEs in policy making, law enforcement and the ongoing digital transformation of the sector.
Keywords: cybersecurity, SMEs, economy, legal framework, risks.

Introduction

It is undeniable that digital autonomy and cyber security have now become a high strategic priority for the European Union (EU) and its Member States. In Latvia, the number of cyber-attacks has increased by 40% since 2022, and attacks on critical infrastructure as well as on public institutions have quadrupled; therefore, the level of cybersecurity threat could be considered to be high. It is often enterprises that are the target of cyber-attacks, thus both risking enterprises resources and becoming 'gateways' to access enterprises customers, including public authorities (Cert.lv., 2024). During the COVID-19 pandemic SMEs had to continuously adapt, including restoring Internet services, understanding cloud services, managing work remotely, etc. This created unprecedented challenges for SMEs, thereby increasing cyber threats and resulting cyber problems. Vulnerabilities in business are manifold. The rapid adoption of new technologies in the business environment such as cloud computing, artificial intelligence, blockchain, big data, etc. has not only accelerated the pace of digital transformation in SMEs but has also created a number of unprecedented challenges. During the digital transformation, SMEs could be more vulnerable and exposed to cyber-attacks. Moreover, it is cybersecurity that is crucial for business continuity, thereby resulting in the technological leap (Saeed et al., 2023). Cybersecurity risks range from data breaches to sophisticated cyber-attacks, with far-reaching and devastating impacts on business operations. Accordingly, a holistic understanding and strategic approach is essential to mitigate cyber threats (Benjamin et al., 2024). Therefore, this study aims to identify and analyse the cybersecurity risks and challenges for SMEs during their digital transformation from a legal and economic perspective.

Materials and Methods

The following research methods were employed to achieve the research aim: monographic and descriptive, which were based on a literature review to collect and analyse legal and economic literature on cybersecurity requirements of SMEs, risks and future challenges.

The research analysed research papers, conference proceedings, and reports by public authorities and performed a content analysis focused on cybersecurity risks in the SME sector. Based on the findings, the research developed a theoretical discussion, identifying the main risks affecting the cybersecurity of SMEs. The legal analysis method was employed to collect, organize and analyse regulatory legislation and policy documents at the national and EU levels (Hamzani et al., 2023).

Various methodologies are applied to make effective decisions. One such method is a questionnaire, which is considered one of the most effective research methods (QuestionPro, [n.d.]). The research used an empirical research method – a sociological survey –, and the results of the survey were analysed using statistical data analysis. Recent studies have demonstrated that enhancing security measures is only attainable through the advancement of digital competencies (Nyikes et al., 2022). The sociological survey was conducted with the aim to explore employees' evaluation of their digital literacy and to examine their motivation to acquire new knowledge and skills. The survey period was from April 2024 to June 2024, and a total of 152 respondents: 125 females and 27 males were interviewed, IBM SPSS software was used for statistical data analysis, while for calculation and analysis of statistical indicators – sampling and inferential statistical methods, including 'descriptive statistics', 'crosstabulation', and 'chi-square test' were used (Kristapsone, 2020).

Results and Discussion

1. Cybersecurity landscape for SMEs in the context of digital transformation

As regards the subject of cyber security, it should be mentioned that the Contact Committee of the EU explains the term cyber-attack as *'an attempt in cyberspace to endanger or destroy the confidentiality, integrity and availability of data or a computer system'* (Contact Committee, 2020). The term digital transformation is used to describe the introduction of digital solutions into business, which can lead to significant change and impact in a variety of areas, including business processes, customers, target markets and user experience (Saeed et al., 2023).

In the history of cyber-attacks, there are several famous cyber-attacks to note, one of the most dangerous being WannaCry, which blocked 200,000 computers in 150 countries using the Windows operating system in 2017. The result was encrypted data and a ransom demanded from the victim. In 2015, a cyber-attack on the Ukrainian electricity grid caused 230,000 people to experience a power outage. The cyber-attack involved phishing, whereby an employee receiving an email opened an infected Microsoft file with malware, thereby having irreparable consequences (Ahmad, 2023).

Arroyabe, Arranz and Arroyabe, Arroyabe have noted that SMEs often do not allocate enough resources to effective cybersecurity measures. The reason is a lack of understanding of the potential risks and the value of the investment. Therefore, best practices, regulatory requirements, complexity of cyber threats and organisational awareness are regarded as key drivers of cyber security in enterprises (Arroyabe et al., 2024). Ambreen, Jain, Yadav and Loonkar argue that raising awareness among SME decision-makers of the potential consequences of cyber-attacks on SMEs should be prioritised, with an emphasis on the responsibility of managers (Ambreen et al., 2024).

The 2024 Global Cyber Outlook focuses on two important areas of cyber security. First, it highlights the growing inequalities in cyberspace that have a significant impact on SMEs, noting several reasons such as early adoption of transformative technologies, limited access to cybersecurity services, legislation development, etc. Second, it highlights the impact of advanced technologies such as generative AI and large language models. Accordingly, a responsible approach to the introduction of advanced technologies is essential, involving the timely reinforcement of the systems supporting them (World Economic Forum, 2024a).

SMEs are recognised as a primary catalyst for economic growth and social development on a global scale. Wang points out that risks such as supply chain disruptions (technological, security and organisational) are typical for SMEs in the context of digital transformation. Thus, a set of measures such as the implementation of cybersecurity governance, security management tools, and supporting measures including hybrid training strategies to educate employees on the impact and potential of technology are essential to mitigate the risks (Wang, 2023). Romi points out that digital skills in the workforce are an essential aspect of regional economic development. Accordingly, digital competencies are necessary and imperative in using various digital opportunities such as ICT design and development, manufacturing, support and service, marketing, etc. (Romi, 2024). The 2024 Fortinet study concluded that to combat cyber-attacks, human resources need not only cyber security tools but also a certain set of skills. At the same time, the integration of innovative technologies based on a continuous build-up of knowledge and skills is an essential aspect of the fight against cyber threats (Fortinet, 2024). Annarelli and Palombi argue that the advent of digitalisation in business has accelerated a paradigm shift in the threat posed by cyberspace. Moreover, cyber resilience in the enterprise is fostered by, among other things, a continuous build-up of knowledge about the unique features of the latest digital technologies (Annarelli & Palombi, 2021).

A research study by Chidukwani, Zander and Koutsakis is dominated by concerns that cyber risks are evolving faster than digital technologies. As a result, problems are exacerbated by inexperience in the use of security technologies. In addition, SMEs' lack of resources to develop their networks also makes them easy targets for attackers. Therefore, social engineering is regarded as the most common form of attack against SMEs, including phishing attacks, hacking as data theft, malware, etc. (Chidukwani et al., 2022).

Luukkonen and Sönmez believe that phishing and social engineering are the main external threats that pose a potential attack on SMEs. They regard poor device and password protection, inadequate risk assessment and training, low skills and cyber hygiene culture as internal threats (Luukkonen & Sönmez, 2023).

Rawinadaran, Jayal, Prakash and Hewage have estimated that SMEs are most often confronted with three cyber security problems: first, malware attacks that cause damage to their networks and computer systems; second, phishing attacks; and third, ransomware attacks that lock down computer systems until a ransom is paid. Therefore, effective cyber security requires an understanding of the threats and their prevention (Rawindaran et al., 2023). Alahmari and Duncan revealed in their research study that 333 out of 612 SMEs in the UK were victims of a cyber-attack in 2018, thereby pointing out that cybersecurity risk management was essential for SMEs. They noted five sequential aspects as important, namely threats, behaviours, practices, awareness and decision-making (Alahmari & Duncan, 2020). Cybersecurity risks in digital transformation highlight the need for a regulatory framework with common cybersecurity

requirements, standards and liability thresholds addressing the specific needs of SMEs.

2. Scope and impact of the regulatory framework for cybersecurity for SMEs

2.1. EU legal regulations and their implications at the national level

One of the EU initiatives is to achieve the same high level of security for information systems across the EU, therefore the NIS Directive (European Parliament and..., 2016), adopted in 2016, introduced security measures and obligation to report security incidents. The improvements made were successful, yet given the volume, number and frequency of cybersecurity incidents, the risk of serious threats to the operation of networks and information systems is still increasing daily (Schmitz-Berndt, 2023). On 18 October 2024, the EU Directive NIS 2 replaced the original 2016 Directive, leaving Member States ill-prepared to face changing and emerging cybersecurity challenges (Vandezande, 2024).

The revised Directive, extends the regulation by the 2016 NIS Directive and sets stricter cyber security requirements for service providers (European Commission, 2024). For example, improving attack and risk management measures in SMEs if it is SMEs that supply products to larger enterprises. In this case, an attack on the supply chain can affect SMEs as well as larger enterprises (European Parliament and..., 2022). The requirements set by the Directive apply to 'essential' public and private entities such as food manufacturing, digital and postal services, etc., as well as 'important' entities such as banking, energy and manufacturing services, etc. (Ministry of Defence, 2023). Annexes I and II of the NIS2 Directive list in sequence both the essential and the important fields and the breakdown of fields to which the requirements of the Directive apply (European Parliament and..., 2022). The Member States are given an opportunity to specify which SMEs are essential or important for the economy or society of their Member State (DIGITALEUROPE, 2021), thereby identifying the fields or services that should be considered critical (The State Chancellery, 2025). Therefore, the requirements set by the Directive are also applicable, inter alia, to SMEs operating in the specified fields of activity.

To meet the requirements set by the NIS2 Directive and to implement the goals set by the Strategy in Latvia, the National Cyber Security Law (National Cybersecurity Law, 2024) came into force on 1 September 2024, replacing the previous Law on the Security of Information Technologies. The law applies to essential and important service providers operating in the energy, transport, health, banking and financial market industries and, based on a national initiative, also covers the security services industry and scientific institutions (National Cybersecurity Law, 2024). The requirements also apply to critical ICT infrastructures: bridges, hospitals, electricity infrastructure or port facilities. For example, an SME owning information technology systems in a critical industry needs to maintain the systems, or an SME that cooperates with larger enterprises operating in that industry. In this case, SMEs also have to comply with the requirements. The preamble to the NIS Directive 2 states that every EU Member State, including Latvia, should address the cybersecurity needs of SMEs in their cybersecurity strategies. Given the large number of SMEs in the business and industrial markets, it has been recognised that it is SMEs that face the greatest difficulty in adapting to working online and being targeted in supply chain attacks. Therefore, the strategies should include addressing such challenges and helping SMEs specifically (European Parliament and..., 2022). Based on the NIS2 Directive, as well as other legal acts, the Latvian Cyber Security Strategy 2023-2026 has been developed to contribute to cyber security in Latvia.

The most recent changes to strengthen security in the electronic environment are governed by the Cyber Resilience Act, which entered into force on 10 December 2024. It is the key piece of legislation to date (in addition to the NIS2 Directive referred to above and the Cybersecurity Act referred to below) in the EU aimed at protecting consumers and enterprises that have purchased hardware products with digital components or software (European Commission, 2025b). It is consumers who are faced with the choice of a digital product who will be able to make sure that cybersecurity is a general priority. According to the European Council, the requirements set by the Act are aimed at simplifying the identification of products with certain security features (World Economic Forum, 2024b).

Since the EU Cybersecurity Act came into force on 27 June 2019, this EU law also applies to SMEs. It aims to achieve a high level of cyber resilience and confidence by empowering ENISA with new powers needed to achieve its goals and objectives. The Agency's Advisory Group includes, among others, recognised experts from industry stakeholders, including SMEs (European Commission, 2024). In light of the above, for example, the Agency issued a report in 2021 'Cybersecurity for SMEs – Challenges and Recommendations'. ENISA has identified the following main cybersecurity challenges for SMEs: first, a low awareness of cybersecurity in general; second, insufficient protection of critical and sensitive information, budget problems, a lack of ICT cybersecurity expertise and personnel, a lack of appropriate guidelines, and challenges related to working online, electronic devices and low management support (European Union Agency…, 2021). The Agency's recommendations include measures such as employee training, regular software updating and incident response planning. Besides, to strengthen the overall security situation, each Member State is called upon to support SMEs by providing them with tailored resources, as well as to facilitate

information sharing (European Union Agency…, 2021). In addition, as stated by the European non-profit organization Small Business Standards (SBS), SMEs need to be provided with guidelines for understanding key legal acts relating to cybersecurity as well as the way they interrelate. For example, the Cyber Resilience Act and the NIS2 Directive. This is aimed, among other things, at reducing costs concerning potential outsourcing (Small Business Standards, 2023).

Although the report contains recommendations for the enhancement of cybersecurity, in March 2023, the Agency released a tool specifically designed to help SMEs to assess their levels of preparedness for cybersecurity. The tool performs two functions. First, a cybersecurity assessment, which determines the enterprise level of cybersecurity, considering its size, field, budget and other factors, and compares it with similar enterprises. The second function involves designing a personalised action plan, which in turn offers to create a cybersecurity improvement plan with particular steps based on current best cybersecurity practices (European Union Agency…, 2023).

2.2. Future AI-related challenges for SMEs

The digital transformation of SMEs has a major impact on any government policy; therefore, support systems are needed to implement AI in SMEs and overcome financial barriers (Schwaeke et al., 2024).

A legal act that should be specifically mentioned in relation to cybersecurity protection for SMEs is the first comprehensive legal act concerning artificial intelligence (AI) in the world (European Commission, 2025c), the AI Act, which will be fully applicable from 2 August 2026. For example, Article 62 of the Act requires the Member States to provide SMEs, including start-ups, priority access to a safe testing environment for new technologies and services, the so-called 'regulatory sandbox', and to promote understanding of the Act's provisions and the application through support and advice, training, the development of common information platforms, etc. (European Parliament and..., 2024). More specific requirements set by the Act, for example, relate to the development of standardised contractual clauses and other templates specifically for high-risk AI systems, which can be implemented by the European AI Office (European Parliament and..., 2024). It should be noted that the first provisions arising from the Act regarding prohibited AI practices that threaten fundamental rights and the security of citizens, as well as AI literacy, are applicable as of 2 February of 2025 (European Commission, 2025a).

Research shows a number of benefits of AI for SMEs. For example, higher efficiency, better decision-making, as well as overall customer satisfaction with marketing, risk management and human resources. However, effectively meeting the requirements specifically in the SME environment has been recognised as a challenge to address problems such as aligning decisions and processes, as well as gaining acceptance from the whole business team. It is the legal uncertainties associated with the introduction of AI into SMEs that necessitate a tool allowing the SMEs to be aware of the relevant regulatory framework (Schwaeke et al., 2024). For example, based on the Digital Decade 2023 report on the digital transformation performance of Latvia, it could be concluded that only 52% of SMEs in Latvia had achieved a basic level of digital intensity in 2022, which was relatively low compared with the EU average of 69% and the Digital Decade target of 90% (Ministry of Environmental..., 2024). In order to transpose the provisions of the AI Act for SMEs, it is necessary for the European Commission to provide guidance, while at national level the EU Member States will have to undertake extensive harmonisation and adaptation processes.

It is undeniable that in practice, the requirements for SMEs that the AI legal framework requires to be met are financially costly. However, the preamble of the AI Act states that it is the new medium-sized enterprises that need to have access to support measures to comply with the Act, not only due to a lack of legal resources but also due to a lack of training (European Parliament and..., 2024). The research study highlights that the cost ceiling for AI is determined both by the IT expertise required in this industry and by skilled human resources. The case law examined by the European Commission showed that SMEs undoubtedly incurred higher costs in implementing AI requirements than large enterprises did; however, since SMEs are accustomed to using third-party services, additional expenses should be considered business-as-usual (BAU) (Sommer et al., 2023).

2.3. Empirical research findings on the role of the human factor in SMEs

From an economic perspective, there are two main causes of challenges to overcome to achieve optimal cybersecurity standards in case of market imperfections. First, the fact that consumers themselves are largely unable to assess the overall level of cybersecurity of a digital product, thus not making a large monetary investment in a potentially safer option (Chiara, 2022**)**. Half a year ago, a research study found that there was a lack of research on whether various categories of SMEs might perceive investment returns differently (Wilson & McDonald, 2024). Second, a research study on the optimal level of investment in the cybersecurity market concluded that the level of investment was not considered optimal enough (Chiara, 2022**)**. In this respect, the available support and EU co-funding for SMEs in Latvia should be emphasized as a positive step towards providing the necessary support to SMEs at the national level. For example, at the end 2024, an EU grant support programme for enterprises of EUR 20,000-60,000 aimed to strengthen the cyber resilience of enterprises and promote the transformation of cyber security by

facilitating access to cyber security solutions. Accordingly, there were implemented pilot projects on technological solutions or developing and introducing cybersecurity technologies (The Cabinet of..., 2024). Since 2023 in Latvia, support for the digitalization of processes using grants available directly to SMEs has also been implemented through the Investment and Development Agency of Latvia. Funding of up to EUR 10,000 from the European Recovery Fund is granted for the development, implementation or transformation of digital services, products and software applications (Investment and Development…, 2023). For example, for the implementation of administrative, personnel management, sales, data management, transport and logistics, production, quality management etc. processes, the grant programme is planned to be implemented until 31 March 2026 (Investment and Development…[n.d.]).

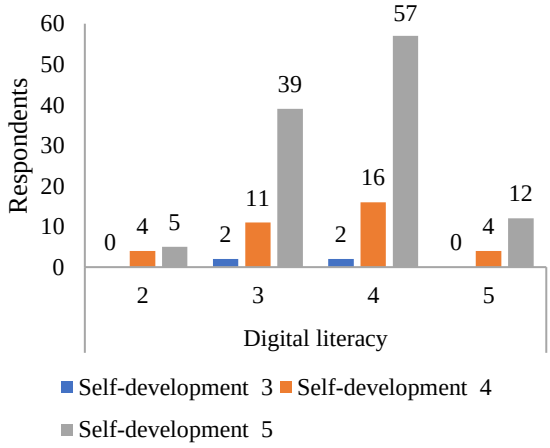
In connection with the aforementioned matter, a sociological study was conducted, the findings of which highlighted the importance of the human factor in cybersecurity. Employees must possess a set of skills, including digital literacy and the continuous renewal of skills and knowledge, in order to act as a cybersecurity shield for the enterprise. The objective of this empirical study was to investigate employees' self-assessment of their digital competence and assess their motivation to acquire new knowledge and skills. A total of 152 respondents were surveyed: salaried employees aged between 18 and 67, including 125 women and 27 men. The respondents were asked to give ratings on a scale from 1 (poor) to 5 (excellent). The question was as follows: 'How would you rate your digital skills'. A frequency analysis of the answers revealed that 49.3% of the respondents rated their digital skills at 4, which indicated some digital competence. At the same time, 34.2% of the respondents rated their digital skills as average (3) and only 10.5% rated their digital skills as excellent (5). Descriptive statistics revealed that the mean score of the respondents' digital skills: Mean = 3.64, Std. Deviation = 0.749, which indicated that the respondents' ratings did not significantly vary, and most of the responses fell into the category of values 3 and 4. At the same time, the results showed that Mode = 4, indicating that the most frequent rating of digital skills by the respondents was 4.

An analysis of the answers to the question: 'How important is personal development and learning new skills throughout your life to you' (see Figure 1, 'self-development') on a scale from 1 (not very important) to 5 (very important) revealed that based on the results of a frequency analysis, the vast majority of 74.3% gave a rating of 5, considering the acquisition of new knowledge very important, while 23% considered it important, and only 2.6% considered personal development and the acquisition of new knowledge less important. Descriptive statistics showed that the mean value of the respondents Mean= 4.72, Std. Deviation = 0.507; therefore, personal development throughout life was considered very important.

Analysing a relationship between the respondents' self-assessment of digital skills and the importance of learning new knowledge and based on the results of a chi-square test, the authors found that since $\chi^2 = 3.40 < \chi^2_{0.05} = 12.59$, df =6, Sign.=0.757 n=152, the null hypothesis could not be rejected; therefore, there were no statistically significant differences between the respondents' answers about digital skills and the importance of learning new knowledge. The results showed that we could not state that the respondents' self-assessments of their digital skills statistically related to their ratings of the need to acquire new knowledge throughout life. Based on the results of a cross-tabulation analysis, the following trend was identified: 113 out of 152 respondents rated learning and developing themselves throughout life as very important (5), 39 respondents (34.5%). Figure 1 rated their digital skills at 3 and 57 respondents (50.4%) gave a rating of 4 and 12 respondents gave a rating of 5. The following trend could be identified: the respondents who considered self-development, including lifelong learning, as very important, were more likely to rate their digital skills as medium and high.

Figure 1

Distribution of the respondents' self-assessment of digital skills according to the importance of knowledge acquisition, 2024



Source: authors' construction based on the results of a questionnaire survey and SPSS data analysis, 2024.

The sociological survey revealed that the vast majority of the respondents (74.3%) rated lifelong learning as very important. This could indicate the readiness of human resources for continuous renewal of skills. However, the average rating of digital skills was 3.64. It could be stated that the ratings of skills by the respondents were moderately high, which indicated not only the acceptance of innovative technologies but also their usage. Kruger and Dunning have explained

in their research study that people tend to overestimate their skills. Accordingly, the skills that increase competence in a specific field often coincide with the skills that are necessary to rate such competence in themselves and others (Dunning & Kruger, 1999). Although there were no statistically significant differences between the answers given by the respondents, the following trend was found: the respondents who rated lifelong learning as very important more often rated their digital skills as medium or high.

The sociological research analysis confirms the influence of the human factor in improving cybersecurity. It can be said that the majority of respondents rated their digital skills with an average score of 3.64, which is medium-high. In addition, 74.3% of respondents considered lifelong learning to be very important, confirming a high motivation to acquire new knowledge and skills. There was also a tendency for respondents who rated lifelong learning as more important to have higher self-rated digital skills.

Conclusions

1. SMEs are considered particularly vulnerable to cyber resilience. Insufficient financial and human resources, a lack of support systems and uncertainty regarding the interpretation of regulatory requirements in practice are among the main cybersecurity risks and threats to SMEs.
2. MEs are strategically important entities because SMEs can be market actors in the supply chain and be connected with larger enterprises at the municipal or national level. Therefore, it is necessary to pay increased attention to the application of proportionate requirements specifically to the cyber resilience SMEs arising from EU legislation.
3. Effective threat management in SMEs involves the management's understanding of and skills in dealing with threats, technology integration based on knowledgeable human resources and safe risk management. To achieve this, the results of the sociological survey revealed that 74.3% of the respondents considered lifelong learning to be very important. This indicated the readiness of human resources for a continuous build-up of their skills. As a result, the competence of employees will be increased, and consequently mistakes and lack of knowledge will be reduced, which will contribute to the cybersecurity shield in the enterprise.
4. EU and national institutions have already provided the necessary support for SMEs to adapt the requirements of legal acts to practice, e.g., financial resource opportunities, including grant programmes and cybersecurity assessment tools, etc. However, to guarantee uniform, secure and effective cyber resilience, as well as to meet the requirements set by the relevant legal acts, more effort is needed to guarantee real support in the long term.

References

Ahmad, Z. (2023). Famous cyber-attacks in the history of cyber security. *International Journal of Advance Research, Ideas and Innovations in Technology*, *7*(6). https://www.ijariit.com/manuscripts/v7i6/V7I6-1281.pdf

Alahmari, A. & Duncan, B. (2020). Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. *International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1-5. https://doi.org/10.1109/CyberSA49311.2020.9139638

Ambreen, L., Jain, M., Yadav, R. K., & Loonkar, S. (2024). Effective cybersecurity risk management practices for small and medium-sized enterprises: A comprehensive review. *Multidisciplinary Reviews*, 6. (Supplementary Issue: World Conference on Multidisciplinary Research & Innovation WCMRI). https://doi.org/10.31893/multirev.2023ss080

Annarelli, A. & Palombi, G. (2021). Digitalization capabilities for sustainable cyber resilience: A conceptual framework. *Sustainability*, *13*(23), Article 13065. https://doi.org/10.3390/su132313065

Arroyabe, M. F., Arranz, F. A., Arroyabe, I. F., Arroyabe, J. I. F. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. *Technology in Society*, 78, Article 102670. https://doi.org/10.1016/j.techsoc.2024.102670

Benjamin, L. B., Adegbola, A. E., Amajuoyi, P., Adegbola, M. D., & Adeusi, K. B. (2024). Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. *Global Journal of Engineering and Technology Advances*, *19*(2), 134–153. https://doi.org/10.30574/gjeta.2024.19.2.0084

Cert.lv. (2024). *The number of cyberattacks in Latvia has increased significantly – the highest figure in the last 2 years.* https://cert.lv/lv/2024/09/butiski-pieaudzis-kiberuzbrukumu-skaits-latvija-augstakais-raditajs-pedejo-2-gadu-laika

Chiara, P. G. (2022). The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. *Int. Cybersecurity. Law Rev.* 3, 255–272. https://doi.org/10.1365/s43439-022-00067-6

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. *IEEE Access*, 10, 85701–85719. https://doi.org/10.1109/ACCESS.2022.3197899

Contact Committee. (2020). *Cybersecurity in the EU and its Member States*. https://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_LV.pdf

DIGITALEUROPE. (2021). *DIGITALEUROPE position on the NIS2 Directive*. https://www.digitaleurope.org/resources/digitaleuropes-position-on-the-nis-2-directive/

European Commission. (2024). *First implementing rules on cybersecurity of critical entities and networks under the NIS 2 Directive.* https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5342

European Commission. (2025a). *First rules of Artificial Intelligence Act are now applicable*. https://digital-strategy.ec.europa.eu/en/news/first-rules-artificial-intelligence-act-are-now-applicable

European Commission. (2025b). *Cyber Resilience Act.* https://digital-strategy.ec.europa.eu/lv/policies/cyber-resilience-act

European Commission. (2025c). *Artificial Intelligence Act.* https://digital-strategy.ec.europa.eu/lv/policies/regulatory-framework-ai

European Parliament and the Council. (2016). Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*, L194 (06.07.2016.). https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:32016L1148

European Parliament and the Council. (2022). Directive (EU) 2022/2555 measures for a high common level of cybersecurity across the Union. *Official Journal of the European Union*, L333, (14/12/2022). https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?qid=1706268746905&uri=CELEX%3A32022 L2555

European Parliament and the Council. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). *Official Journal of the European Union*, L 2024/1689 (12.07.2024.). https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=OJ:L_202401689

European Union Agency for Cybersecurity. (2021). *Cybersecurity for SMEs. Challenges and Recommendations*. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Cybersecurity%20for%20SMES%20Challenges%20and%20Recommendations.pdf

European Union Agency for Cybersecurity. (2023). *The European Union Agency for Cybersecurity (ENISA) releases a tool to help Small and Medium Enterprises (SMEs) assess the level of their cybersecurity maturity*. https://enisa.europa.eu/news/diagnose-your-sme2019s-cybersecurity-and-scan-for-recommendations

Fortinet. (2024). *2024 Cybersecurity Skills Gap Global Research Report*. https://www.fortinet.com/content/dam/fortinet/assets/reports/2024-cybersecurity-skills-gap-report.pdf

Hamzani, A. I., Widyastuti, T. V., Khasanah, N., & Rusli, M. H. M. (2023). Legal research method: Theoretical and implementative review. *International Journal of Membrane Science and Technology*, *10*(2), 3610–3619. https://doi.org/10.15379/ijmst.v10i2.3191

Investment and Development Agency of Latvia. (2023). Support for the Digitalization of Processes in Business. https://www.liaa.gov.lv/lv/programmas/atbalsts-procesu-digitalizacijai?utm_source=https%3A%2F%2Fwww.google.com

Investment and Development Agency of Latvia. [n.d.] *Support for Digitalization. Business.gov.lv.* https://business.gov.lv/atbalsta-programmas/atbalsts-digitalizacijai

Kristapsone, S. (2020). Data Management in SPSS. In: Kristapsone, S. (Eds.) *Statistical Analysis Methods in Researc*h. Riga, Drukātava Ltd.

Kruger, J. & Dunning, D. (1999). Unskilled and unaware of it: How difficulties in recognizing one's own incompetence leads to inflated self-assessments. *Journal of Personality and Social Psychology, 77*(6), 1121–1134. https://doi.org/10.1037/0022-3514.77.6.1121

Luukkonen, O. A. & Ülgen Sönmez, Y. (2023). Cybersecurity for small and medium-sized businesses. *Journal of Sustainable Economics and Management Studies, 3*(1), 21–38. https://dergipark.org.tr/en/pub/ecoman/issue/80789/1334298#article_cite

Ministry of Defence. (2023). *Cybersecurity Strategy of Latvia for 2023-2026.* https://www.mod.gov.lv/sites/mod/files/document/Latvijas%20kiberdrošības%20stratēģija%202023.-2026.gadam_.pdf

Ministry of Environmental Protection and Regional Development of the Republic of Latvia. (2024). *Information report: Digital Decade Strategic Roadmap for Latvia until 2030 (draft).* https://www.varam.gov.lv/lv/media/38076/download?attachment

National Cybersecurity Law. (2024). *Latvijas Vēstnesis 128A (04.07.2024.).* [Official Publisher of the Republic of Latvia]. https://likumi.lv/ta/id/353390

Nyikes, Z., Kovács, T. A., Honfi, V. S., & Illési, Z. (2022). Digital Competence and Security Awareness from the Perspective of Sustainability. In: Kovács, T. A., Nyikes, Z., Fürstner, I. (Eds.) *Security-Related Advanced Technologies in Critical Infrastructure Protection.* NATO Science for Peace and Security Series C: Environmental Security. Springer, Dordrecht. https://doi.org/10.1007/978-94-024-2174-3_12

Rawindaran, N., Jayal, A. Prakash, E., & Hewage, C. (2023). Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales. *International Journal of Information Management Data Insights*, *3*(2), Article 100191. https://doi.org/10.1016/j.jjimei.2023.100191

Romi, I. M. (2024). Digital Skills Measures for Digitalization-An Aggregative Analysis. *Pakistan Journal of Life and Social Sciences 22*(1), 971-971. https://doi.org/10.57239/PJLSS-2024-22.1.0067

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors*, *23*(15), 6666. https://doi.org/10.3390/s23156666

Schmitz- Berndt, S. (2023). Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS2 Directive. *Journal of Cybersecurity*, *9*(1), Article tyad009. https://doi.org/10.1093/cybsec/tyad009

Schwaeke, J., Peters, A., Kanbach, D. K., Kraus, S., & Jones, P. (2024). The new normal: The status quo of AI adoption in SMEs. *Journal of Small Business Management*, 1–35. https://doi.org/10.1080/00472778.2024.2379999

Small Business Standards. (2023). *SBS position paper on the Cyber Resilience Act*. https://sbs-sme.eu/wp-content/uploads/2024/01/SBS-Position-Paper_CRA_FINAL.pdf

Sommer, M., Stjepandić, J., Stobrawa, S., & von Soden, M. (2023). Automated generation of digital twin for a built environment using scan and object detection as input for production planning. *Journal of Industrial Information Integration*, 33, Article 100462. https://doi.org/10.1016/j.jii.2023.100462

State Chancellery. (2025, January 17). *Draft law of the National Cybersecurity Law (20/12/2022).* https://tapportals.mk.gov.lv/annotation/d7803af8-e515-43c6-b0db-61c39a0da17e

The Cabinet of Ministers for the republic of Latvia. (2024). The regulation of the Cabinet Regulation of Ministers No. 139 of 27 February 2024 Implementation Regulation for the European Cybersecurity Competence Centre Grant Programme 'Cybersecurity Transformation of Small and Medium-sized Enterprises' for the Planning Period 2021–2027. *Latvijas Vēstnesis,* 45, (04/03/2024). https://likumi.lv/ta/id/350225

Vandezande N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review*, 52, Article 105890. https://www.sciencedirect.com/science/article/abs/pii/S0267364923001000

Wang, Z. (2023). Digital Transformation and Risk Management for SMEs: A Systematic Review on Available Evidence. *Advances in Economics, Management and Political Sciences*, 65, 209-218. https://doi.org/10.54254/2754-1169/65/20231639

Wilson, M. & McDonald, S. (2024). One size does not fit all: exploring the cybersecurity perspectives and engagement preferences of UK-Based small businesses. *Information Security Journal: A Global Perspective*, *34*(1), 15–49. https://doi.org/10.1080/19393555.2024.2357310

World Economic Forum. (2024a). *Global Cybersecurity Outlook 2024*. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

World Economic Forum. (2024b). *EU adopts cyber resilience act- and other cybersecurity news to know this month.* https://www.weforum.org/stories/2024/10/eu-cyber-resilience-act-cybersecurity-news-october-2024/

QuestionPro. [n.d.]. *Survey research definition*. https://www.questionpro.com/blog/survey-research/