Journal of Information Systems Engineering and Management
2025, 10(12s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Contemporary Strategies for Managing Organisational Information Security

Anatolii Benzar[1], Yuliia Kovalenko[2], Artem Taranenko[3], Olha Balynska[4], Igor Balynskyi[5]
[1]*Department of Economics and Management, The Zakhidnodonbaskyi Institute of the Private Joint-Stock Company "Higher Education Institution "Interregional Academy of Personnel Management", Pavlohrad, Ukraine*
[2]*Department of Cyber Security, Faculty of Computer Sciences and Technologies, National Aviation University, Kyiv, Ukraine*
[3]*The Institute of Security, PJSC "Higher Educational Institution" Interregional Academy of Personnel Management, Kyiv, Ukraine*
[4]*Research Laboratory for the Study of Problems of Combatting Human Trafficking, Educational and Scientific Institute for Training Specialists for Criminal Police Units, Lviv State University of Internal Affairs, Lviv, Ukraine*
[5]*Department of Journalism, Advertising and Public Relations, King Danylo University, Ivano-Frankivsk, Ukraine*

ARTICLE INFO

Received: 15 Nov 2024

Revised: 28 Dec 2024

Accepted: 14 Jan 2025

ABSTRACT

Introduction: Due to the growing number and complexity of cyberattacks on organisations in various sectors of the economy, there is an urgent need to find the most modern approaches to information security management. Outdated approaches and counteracting and combating information incidents cannot fully protect organisations from new threats.

Objectives: The article aims to highlight the main trends and features of implementing modern approaches to information security management in organisations.

Methods: The research methodology is based on a descriptive-analytical design and a mixed approach, combining theoretical aspects of information security management and analysis of secondary data on the status and features of implementing modern approaches to information security management in organisations.

Results: The results show that the growing number and complexity of cyber attacks on organisations lead to significant operational, economic, and reputational risks and losses. As a result, more and more companies are implementing approaches to information security management, among which the most common are holistic and risk-based. Legislative changes in the EU in personal data protection have also been one of the main drivers of information security.

Conclusions: The practical value of the work lies in the systematisation of existing trends and peculiarities of implementing modern approaches to the information security management of organisations.

Keywords: information, information law, communication, human rights, information security, restriction of the right to disseminate information.

INTRODUCTION

The dynamic use of information technology and data in the management of organisations has created numerous opportunities for business development. At the same time, new risks and threats arise in the field of information security, and their complexity increases. In various organisations, information security risks concerning their innovative development are highly relevant and important[1]. In this regard, the issues of information security (IS) are considered not only in the technological context but also the researchers' attention is growing to the study of theoretical and practical management principles in this area of organisations' activities [2].

Thus, organisations operate in an area where operational, economic, and reputational problems may arise. According to Jerman-Blažič and Bojanc [3], as IS risks increase, investments in security and data protection services increase, and economic problems increase accordingly. Protecting enterprise resources requires significant investment in IS. Investing in IS is also associated with introducing legislative changes in this area [4]. Economic problems and losses

can also arise due to other reasons in organisational IS. For example, a credit bureau in America paid over USD 1 billion in fines to about 150 million consumers after a data breach in 2017. From 2004-2023, the US financial sector suffered more than 20,000 cyberattacks, which resulted in $12 billion in losses [5].

According to information, in the last twelve months of 2024, 70% of UK businesses received fines for data breaches over £100,000. Among UK companies, 79% were affected by information security incidents (deepfakes) caused by third-party suppliers or their partners. Compared to 2023, the number of affected companies has increased by 20% [6]. According to the U.S. Identity Theft Resource Centre, more than 1 billion victims of cyberattacks for data theft were recorded in the first half of 2024, an increase of 490% compared to 2023 [7]. According to a survey conducted by KPMG in May 2024, 40% of cybersecurity executives from 200 companies surveyed reported cyberattacks, and 76% expressed concern about the growing sophistication of new cyber threats. Threats include organised cybercriminal groups, hackers, employees and contractors of organisations [8].

Therefore, several risks exist in the field of information security, such as data leakage, cyber attacks, and fraud using information and communication tools and technologies. The relevance of researching modern approaches to managing organisations' information security is growing in this regard.

The article aims to highlight the main trends and peculiarities of implementing modern approaches to information security management in organisations.

LITERATURE REVIEW

Information security is defined as maintaining and preserving the integrity, availability, and confidentiality of information by corporate strategies, goals, regulatory, business, and standard requirements of stakeholders [9].

The scientific literature identifies several approaches to information security management [10]. Eloff and von Solms [11] study systematised the main approaches to IS management based on international standards. According to Lee [12], cyber risk management based on different standards should be holistic, considering technical and human aspects. Soomro et al. [2] argue for a holistic approach to information security management. Based on an empirical study, it was found that the following components had a significant impact on the quality of IS management: development and implementation of IS policy; raising staff awareness in the field of IS, training; development of an effective information architecture of the enterprise; management of IT infrastructure of organisations; coordination of business activities with IT, human resources management [2, 13, 14]. The holistic approach is also studied in the publication by Eloff and Eloff [15], particularly the need to establish an IS management system with the following components: policies, standards, codes of practice, guidelines, technologies, legal and ethical issues. Kaushik [16] presents a comprehensive methodology for cybersecurity management based on holistic, reliable, adaptive approaches, which, in particular, involve integrating machine learning and blockchain technologies. The paper presents the results of implementing a holistic approach to cybersecurity management in Portuguese SMEs based on the ISO-27001:2013 Standard. In general, the implementation of information security audit processes, their continuous improvement, training, and certification of SME employees are also important within projects to reduce risks and positively impact enterprises' operations [17].

Stewart and Jürjens [1] describe an agile approach to IS governance that involves using flexible tools depending on organisations' individual needs. Flexibility has a positive impact on IS governance but requires enterprises to maintain dynamic compliance processes with this approach by introducing compliance standards, closing gaps, and monitoring the integration of the approach [1].

Less commonly used in IS management are preventive approaches [18] and compulsory control over information systems [19].

Fenz et al. [20] consider approaches to IS risk management, such as asset inventory, countermeasures, asset valuation, risk forecasting, knowledge sharing, and weighing risks against losses. Jerman-Blažič and Bojanc [3] consider the approach based on IS risk modelling to minimise the risks of potential cyberattacks and losses of organisations. This approach is based on identifying ICT system assets, threats, vulnerabilities, and procedures to select the most optimal investments in the required security technologies. Meszaros and Buchalcevova [21] also present an approach to security management based on threat and risk management. Such approaches are relevant in the context of organisations' budgetary constraints, as they allow for the identification of asset risks and threats that require the most investment in IS [4]. According to Alahmari and Duncan [22], the following components are

important in managing the cyber risks of SMEs: impact on threats, staff behaviour, awareness raising, and decision-making. At the same time, as Ganin et al. [23] rightly point out, the approach based on risk management related to information interests usually does not cover all components of organisational management.

In general, the advantages of a holistic approach to information security management include considering all components and aspects of management, building a holistic management system that protects all assets, resources, data, and personnel of the company, and raising its cybersecurity awareness. A flexible approach to management allows organisations to adapt to their needs in the field of information interests protection and choose the most appropriate tools to influence threats (Table 1).

Table 1: Advantages and disadvantages of different approaches to organisational IS management

Approach	**Advantages**	**Disadvantages**
Holistic	Takes into account all components and aspects of organisational IS management Provides for the protection of both information assets and personnel and data Provides opportunities to raise staff awareness of security issues	Requires significant investment Requires organisations to develop an organisational culture of security Requires constant review of legal aspects of implementation
Flexible	Adapts to the needs of businesses Provides the ability to select the most necessary management tools	Requires enterprises to support dynamic processes to comply with this approach It may not take into account other practical management tools that are less flexible but more effective
Approaches to risk management in the field of security	Focuses on the most vulnerable assets and resources of organisations Takes into account key security risks and threats Effective for organisations with budgetary constraints	Requires highly qualified specialists with forecasting and risk modelling skills, while there is a shortage of IS professionals in the labour market

Source: compiled by the author

Thus, despite the above approaches to information security management's apparent advantages, they also have several disadvantages. Therefore, organisations must choose different approaches to managing this activity area, depending on their needs.

METHODS

The study uses a descriptive-analytical design to highlight current trends and features of using approaches to information security management in organisations. At the study's first stage, articles that covered the essence of “approaches to information security management” were selected. As a result, the main advantages and disadvantages of scholars' most discussed management approaches were systematised: holistic, flexible, and risk-oriented. The second stage of the study examines the factors, trends, and peculiarities of approaches used by information security management organisations. At this stage, secondary survey data was collected: 1) on the cyber readiness of companies [24]; 2) the 2024 global survey of information security executives to identify the most threatening cyber risks for companies [25] 3) a survey of company representatives on the state of information security management; 4) a survey of 200 information security executives conducted in May 2024 on cyber threats [8]; 5) ISMS survey [26] on the state of implementation of ISO/IEC 27001. The mixed design of the study allowed for a more comprehensive characterisation of the factors of using holistic and risk-based approaches to information security management.

RESULTS AND DISCUSSION

Information security management in organisations is being transformed by several factors and driving forces in the external environment. Firstly, legal requirements are changing due to new challenges, such as the need to protect personal data, the growth of data collection, and unprecedented data flows between different countries

[27]. We agree that “increased legal requirements and data leakage have further contributed to the need to ensure data privacy” [9].

The legislative changes were aimed at addressing the fragmentation problems in the implementation of legal data protection, legal uncertainty, and significant risks to protecting individuals' data in connection with their online activity. As for organisations, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 sets out the obligations of controllers and processors of personal data to take security measures by the risks associated with data processing. In some instances, controllers are required to report breaches of data protection regulations [28].

The first pan-European cybersecurity rules are defined in the Directive on the Security of Network and Information Systems, which, in particular, defines the obligations of risk management and reporting of existing security incidents by digital service operators/providers [29]. Therefore, the latter must take technical and organisational measures to prevent information security risks, ensure the security of the network and information systems, and prevent and minimise damage to IT systems. First, digital service operators/providers include enterprises that provide services critical to the country's social and economic activity. The Directive also obliges EU member states to adopt national cybersecurity strategies and define methods of public-private cooperation within them[30].

The Directive on the Security of Network and Information Systems in the EU provided for the EU Cybersecurity Agency to certify companies' ICT products, services, and processes. The EU Cybersecurity Act established a pan-European certification system that would give organisations the advantage of having their certified products, services, and processes recognised within the EU. In April 2023, amendments to the EU Cybersecurity Act were adopted, ensuring the creation of certification schemes for “managed security services” in incident response, testing, security audits and consulting. The certification will help to improve the quality of security services provided to organisations by these services [31].

Such legislative changes to the provisions of the EU Cybersecurity Act are justified. For example, financial companies are increasingly using third-party IT service providers. As artificial intelligence technologies become more widespread in the information security space, the use of such services will grow. The external providers are highly specialised in cyber defence, significantly improving operational resilience and the level of protection against threats. For example, in 2023, a ransomware attack on cloud IT service providers caused simultaneous disruptions in the operations of 60 credit unions in the United States [5].

Secondly, the number and complexity of various types of information threats and cyber threats are growing. The latest Hiscox Cyber Readiness Report [24] on company cyber readiness shows an increase in cyber attacks over 2020-2024, with a 36% increase in attacks on small businesses. Average cybersecurity spending by companies increased by 39% between 2020 and 2023.

According to the 2024 Global Chief Information Security Officer Survey, nearly 41% of respondents cited ransomware attacks as one of their organisations' most critical cybersecurity threats. Another 38% of executives worldwide consider malware a severe risk to their organisations' information security. The third threat level is email fraud (36%) (Figure 1).

Thirdly, organisations face several challenges in the context of legislative changes and challenges in information security. The most common problems of organisations in the field of information security include a shortage of professional staff with relevant skills, growing risks of cyber threats, and outdated approaches and methods of information security management. In addition, there are needs such as raising awareness and consciousness among staff about the importance of information security. The latter requires implementing an information security policy in organisations and compliance with its provisions to reduce risks and appropriate behaviour of employees [32]. Raising awareness among staff about information security can be achieved through knowledge sharing [33].

Therefore, companies are implementing modern approaches to information security management both at the expense of their own forces and resources and using the services of highly specialised third-party organisations.

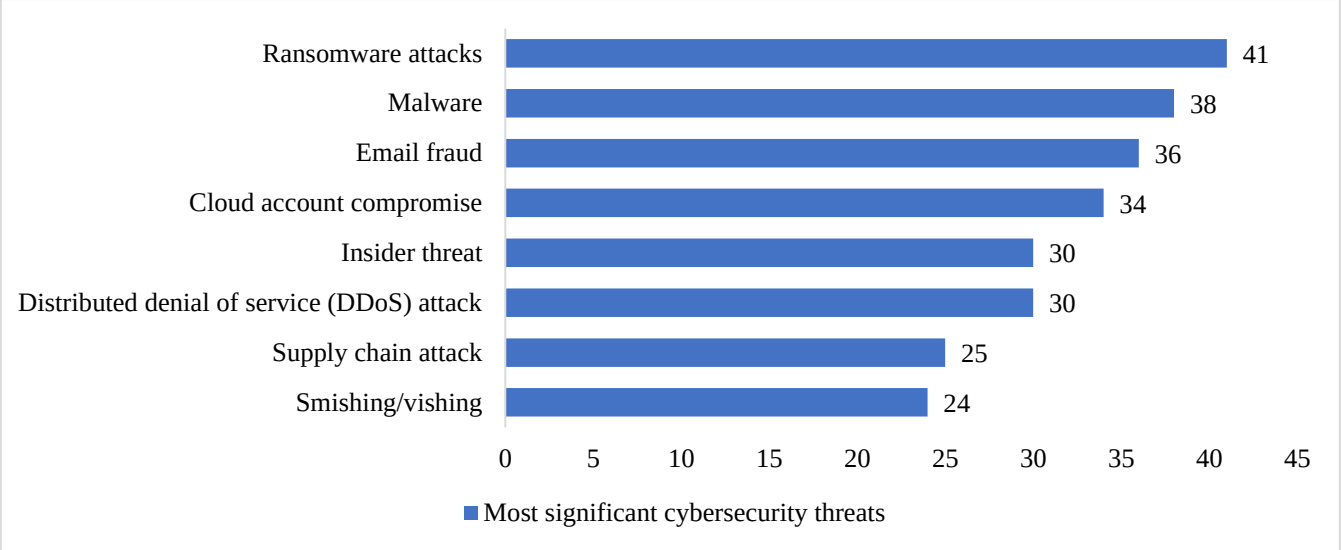

Figure 1: The most significant cybersecurity threats in organisations around the world, according to chief information security officers (CISOs) as of February 2024

Source: Statista [25]

Empirical studies based on the results of surveys of company representatives indicate that companies use a risk-based approach to information security management in their practical activities. Thus, according to a survey of 200 information security executives conducted in May 2024, 76% of them claimed a high level of confidence in understanding their organisations' risk areas and vulnerabilities [8]. This indicates that security executives have at least identified the risks and vulnerabilities associated with information threats to their companies. At the same time, 86% of managers stated that the security operations centre (SOC) was ready to prevent future sophisticated attacks. 90% of executives claimed the security operations centre had complete control over risk areas and vulnerabilities. According to the survey, the current annual budget of the security operations centre is, on average, $14.6 million, of which 37% is allocated to threat prevention and detection [8].

According to Shameli-Sendi et al. [34], “One of the best ways to solve information security problems in the corporate world is a risk-based approach”. According to Shamala et al. [35], most information security risk management methods are based on similar processes, which include defining the assessment area, collecting information, obtaining intermediate risk information, using the collected information to identify security risks, and presenting a security profile of critical information assets.

The use of a holistic approach is also quite common. The ISO/IEC 27001 Standard “Information Security, Cybersecurity and Protection of Privacy” promotes a holistic approach to information security management: checking personnel, existing policies, and technologies. ISO/IEC 27001 enables organisations to establish an information security management system and use a risk management process that can be adapted to the size of the company and its needs [36].

Establishing an information security management system depends on an organisation's needs, objectives, security requirements, organisational processes, size, and structure. Implementing ISO/IEC 27001 helps solve this strategic task and implement a risk-based approach to cyber threat management.

Stoll [9] states that “more than 1.5 million organisations worldwide are implementing a standards-based management system”. The highest implementation of ISO/IEC 27001 requirements is observed among organisations in the information technology sector. This is because certification gives organisations several competitive advantages [37].

In addition, the implementation of the Standard is linked to government policies in some countries. Therefore, the Information Security Strategy of the Republic of Moldova for 2019-2024 envisages compliance with international

standards by organisations, in particular ISO/IEC 27001, to secure data and resources and increase the confidence of foreign investors in organisations in the country [38].

At the same time, according to Kamil et al. [39], the effectiveness of ISO/IEC 27001 in addressing information security issues raises specific questions. This is because stakeholders implementing the requirements of the standard must have a certain level of information security skills. As a result of the different skill levels, the legitimacy of ISO/IEC 27001 performance in different companies in Sweden varies from high to low. According to Culot et al. [40], the implementation of ISO/IEC 27001 leads to several problems in organisations, given the general principles set out in the information security document, and the effectiveness of its implementation is limited to a few pieces of evidence.

Today, the implementation of ISO/IEC 27001 is practically automated to the level of 82% (Figure 2). In particular, the relevant automation programmes make it possible to ensure organisational control at the level of 79%, personnel control at the level of 73%, physical control at the level of 87%, technological control at the level of 80%, and the implementation of additional control measures at the level of 84%.

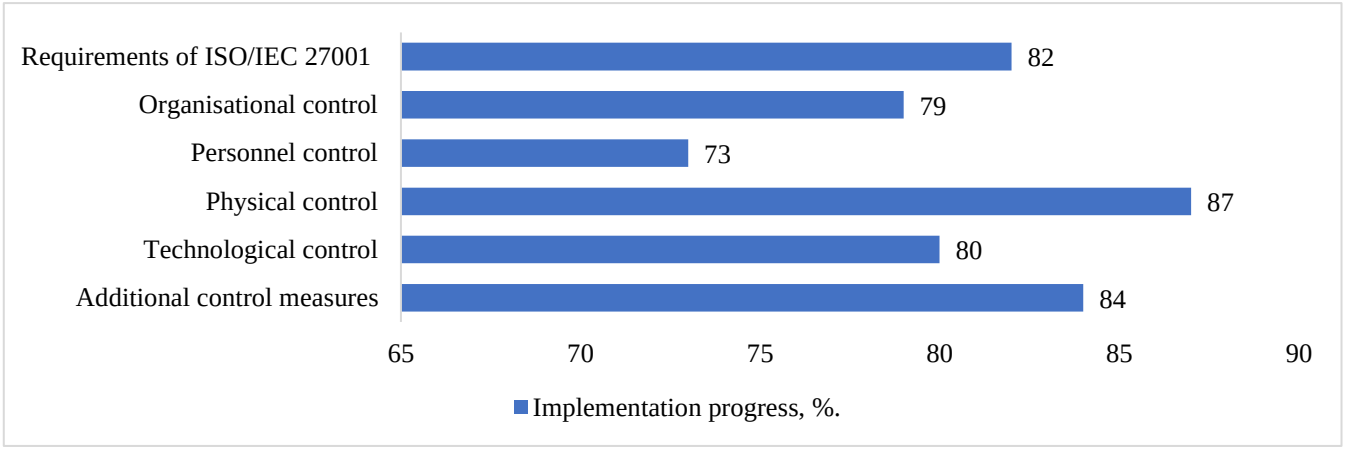

Figure 2: Progress in the implementation of ISO/IEC 27001

Source: ISMS [26]

In addition to the Standard, organisations can use the cybersecurity framework developed by the National Institute of Standards and Technology to implement an information security management plan and programme. This framework includes the following continuous, sequential functions: 1) definition: development of an organisational framework for managing cybersecurity risks for personnel, assets, systems, data; 2) protection: development and integration of protection measures; 3) detection: development and implementation of measures to identify incidents; 4) response: development and implementation of incident response measures; 5) recovery: development and implementation of measures to maintain the sustainability, ability to provide any services of the organisation [41].

Therefore, a generalisation of organisations' practices in information security management indicates that the growing need to protect information interests arises, particularly in response to legislative requirements. Among the latter, it is worth highlighting the requirements for technical and organisational measures to prevent information security risks by digital service operators/providers, as well as certification of ICT products, services, and processes of companies. Due to the growing number and complexity of information threats, measures to improve the cyber readiness of companies are becoming increasingly important. This has become another factor in improving information security management. Organisations are more likely to use a risk-based approach to management in this area, which involves identifying risk areas and vulnerabilities. A holistic approach to management based on ISO/IEC 27001 is quite common in enterprises.

CONCLUSION

The growing number and sophistication of cyberattacks on organisations leads to significant operational, economic, and reputational risks and losses. As a result, more and more companies are implementing approaches to information security management, the most common of which are holistic and risk-based. The first approach allows organisations to establish a holistic information security management system. The second focuses on risk areas and vulnerabilities of organisations and can be implemented as part of the holistic approach. In general, information security management solves the problems of protecting against cyber threats and contributes to creating new competitive advantages for organisations.

Legislative changes in the EU in personal data protection were also one of the main drivers for strengthening information security. In particular, the legal changes defined the obligations of controllers and processors of personal data to take security measures based on the risks associated with data processing. In addition, the legal provisions established obligations for risk management and reporting of existing security incidents by digital service operators/providers. Legal provisions have expanded institutional powers to certify companies' ICT products, services, and processes. As a result, companies have gained competitive advantages in the form of legislative recognition of the quality of their products.

The study is limited by the lack of comprehensive data on the state of implementation of approaches to information security management at the level of individual organisations. This would make it possible to identify companies' practical problems in managing cyber threats.

REFRENCES

[1] Stewart, H.; Jürjens, J. Information security management and the human aspect in organisations. *Information Computer Security*, 2017, *25*(5), 494–534. https://doi.org/10.1108/ICS-07-2016-0054

[2] Soomro, Z. A.; Shah, M. H.; Ahmed, J. Information security management needs more holistic approach: A literature review. *International journal of information management*, 2016, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

[3] Jerman-Blažič, B., Bojanc, R. An economic modelling approach to information security risk management. *International Journal of Information Management*, 2008, *28*(5), 413–422. https://doi.org/10.1016/j.ijinfomgt.2008.02.002

[4] Weishäupl, E.; Yasasin, E.; Schryen, G. Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers Security*, 2018, *77*, 807–823. https://doi.org/10.1016/j.cose.2018.02.001

[5] International Monetary Fund. Rising Cyber Threats Pose Serious Concerns for Financial Stability, 2024. https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

[6] Alliantist. The State of Information Security Report 2024, 2024. https://www.isms.online/state-of-infosec-24/

[7] International Information Systems Security Certification Consortium, ISC2. ISC2 Survey: More Cybersecurity Leadership Training Needed, 2024. https://www.isc2.org/insights/2024/12/isc2-survey-cybersecurity-leadership?queryID=77c010de9f13e0df2cb0b77c783e43f9

[8] KPMG. KPMG Survey: C-Suite Cyber Leaders Optimistic about Defences, but Large Percentage Suffered Recent Cyber Attack, 2024. https://kpmg.com/us/en/media/news/2024-cybersecurity-survey.html

[9] Stoll, M. An information security model for implementing the new ISO 27001. In *Handbook of Research on Emerging Developments in Data Privacy* (pp. 216–238). IGI Global, 2015. https://doi.org/10.4018/978-1-4666-7381-6.ch011

[10] Tvaronavičienė, M.; Plėta, T.; Della Casa, S.; Latvys, J. Cyber security management of critical energy infrastructure in national cybersecurity strategies: Cases of USA, UK, France, Estonia and Lithuania. *Insights into regional development*, 2020, *2*(4), 802–813. https://doi.org/10.9770/ird.2020.2.4(6)

[11] Eloff, M. M.; von Solms, S. H. Information security management: A hierarchical framework for different approaches. *Computers Security*, 2000, *19*(3), 243–256. https://doi.org/10.1016/S0167-4048(00)88613-7

[12] Lee, I. Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, 2021, *64*(5), 659–671. https://doi.org/10.1016/j.bushor.2021.02.022

[13] Tarasenko, O.; Lysenko, S.; Tarlopov, I.; Pidkaminnyi, I.; Verhun, M. Analysis of the competitiveness of higher education institutions in Ukraine in the context of recovery and development after the war. *Multidisciplinary Science Journal,* 2024, *6,* e2024ss0210. https://doi.org/10.31893/multiscience.2024ss0210

[14] Lysenko, S.; Skurativkyi, R. Extended Special Linear group ESL2(F) and matrix equations in SL2(F), SL2(Z) and GL2(Fp). *Wseas Transactions on Mathematics,* 2024, *23,* 643–659. https://doi.org/10.37394/23206.2024.23.68

[15] Eloff, J. H.; Eloff, M. Information security management: a new paradigm. In *Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology*. (pp. 130–136). SAICSIT, 2003. https://www.sis.pitt.edu/jjoshi/courses/is2621/SecManParadigm2.pdf

[16] Kaushik, M. Cybersecurity Management: Developing Robust Strategies for Protecting Corporate Information Systems. *International Journal for Global Academic Scientific Research*, 2024, *3*(2), 24–35. https://doi.org/10.55938/ijgasr.v3i2.75

[17] Antunes, M.; Maximiano, M.; Gomes, R.; Pinto, D. Information security and cybersecurity management: A case study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, 2021, *1*(2), 219–238. https://doi.org/10.3390/jcp1020012

[18] Ahmad, A.; Maynard, S. B.; Park, S. Information security strategies: Towards an organisational multi-strategy perspective. *Journal of Intelligent Manufacturing*, 2014, *25*, 357–370. http://doi.org/10.1007/s10845-012-0683-0

[19] Chen, Y.; Ramamurthy, K.; Wen, K. W. Organisations' information security policy compliance: A stick or carrot approach? *Journal of Management Information Systems*, 2012, *29*(3), 157–188. https://doi.org/10.2753/MIS0742-1222290305

[20] Fenz, S.; Heurix, J.; Neubauer, T.; Pechstein, F. Current challenges in information security risk management. *Information Management Computer Security*, 2014, *22*(5), 410–430. https://doi.org/10.1108/IMCS-07-2013-0053

[21] Meszaros, J.; Buchalcevova, A. Introducing OSSF: A framework for online service cybersecurity risk management. *Computers Security*, 2017, *65*, 300–313. https://doi.org/10.1016/j.cose.2016.12.008

[22] Alahmari, A.; Duncan, B. Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In *2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA*). (pp. 1–5). IEEE, 2020. http://doi.org/10.1109/CyberSA49311.2020.9139638

[23] Ganin, A. A.; Quach, P.; Panwar, M.; Collier, Z. A.; Keisler, J. M.; Marchese, D.; Linkov, I. A multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*, 2020, *40*(1), 183–199. https://doi.org/10.1111/risa.12891

[24] Hiscox Cyber Readiness Report, 2024. https://www.hiscoxgroup.com/cyber-readiness

[25] Statista. The most significant cybersecurity threats in organisations worldwide according to Chief Information Security Officers (CISOs) as of February 2024, 2024. https://www.statista.com/statistics/1350460/cybersecurity-threats-at-companies-worldwide-cisos/

[26] ISMS. The proven path to ISO 27001 success, 2024. https://www.isms.online/solutions/achieve-iso-27001/

[27] Official Journal of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2024a. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[28] European Council. The general data protection regulation, 2024. https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/

[29] Official Journal of the European Union, Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 2024b. https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

[30] European Commission. Directive on Security of Network and Information Systems, 2024a. https://ec.europa.eu/commission/presscorner/detail/el/memo_16_2422

[31] European Commission. The EU Cybersecurity Act, 2024b. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[32] Safa, N. S.; Von Solms, R.; Furnell, S. Information security policy compliance model in organisations. *Computers Security*, 2016, *56*, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

[33] Safa, N. S.; Von Solms, R. An information security knowledge sharing model in organisations. *Computers in Human Behaviour*, 2016, *57*, 442–451. https://doi.org/10.1016/j.chb.2015.12.037

[34] Shameli-Sendi, A.; Aghababaei-Barzegar, R.; Cheriet, M. Taxonomy of information security risk assessment (ISRA). *Computers Security*, 2016, *57*, 14–30. https://doi.org/10.1016/j.cose.2015.11.001

[35] Shamala, P.; Ahmad, R.; Zolait, A.; Sedek, M. Integrating information quality dimensions into information security risk management (ISRM). *Journal of Information Security and Applications*, 2017, *36*, 1–10. https://doi.org/10.1016/j.jisa.2017.07.004

[36] International Organisation for Standardisation. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements, 2024. https://www.iso.org/standard/27001

[37] Šikman, L.; Latinović, T.; Paspalj, D. ISO 27001-Information Systems Security, development, trends, technical and economic challenges. *Annals of the Faculty of Engineering Hunedoara*, 2019, *17*(4), 45–48. https://www.researchgate.net/publication/338585321

[38] Alexei, A. Ensuring information security in public organisations in the Republic of Moldova through the ISO 27001 standard. *Journal of Social Sciences*, 2021, *4*(1), 84–94. https://doi.org/10.52326/jss.utm.2021.4(1).11

[39] Kamil, Y.; Lund, S.; Islam, M. S. Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders' perspective on expectations in private organisations in Sweden. *Information Systems and e-Business Management*, 2023, *21*(3), 699–722. https://doi.org/10.1007/s10257-023-00646-y

[40] Culot, G.; Nassimbeni, G.; Podrecca, M.; Sartor, M. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*, 2021, 33(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202

[41] The National Institute of Standards and Technology. Cybersecurity Framework, 2024. https://www.nist.gov/cyberframework