UDC 005.33
JEL K24, M21

CYBER RESILIENCE KEY METRICS IN SMALL AND MEDIUM-SIZED ENTERPRISES

Sintija Deruma *
BA School of Business and Finance, Riga, Latvia
ORCID iD: 0000-0001-7804-5995

*Corresponding author:
E-mail: sintija.deruma@inbox.lv

Received: 14/11/2024
Revised: 16/01/2025
Accepted: 04/03/2025

DOI: 10.61954/2616-7107/2025.9.1-2

Introduction. Cyber security is a dynamic, human-made environment where information, processes, and technologies converge, making cyber resilience essential for sustainable economic development. Cyber security incidents impede national security, economic stability, and digital transformation, underscoring the need to strengthen cyber capacity globally, especially among small and medium enterprises (SMEs), where each participant's responsibility is essential in the cyber security landscape. Cyber security, being transdisciplinary, necessitates effectively managing the risks, compliance, and socioeconomic impact of cyber security incidents.

Aim and tasks. This study introduces a cyber resilience metrics framework that consolidates security controls by functional areas, aligns them with incident lifecycle stages, and clarifies the purpose and tasks of each stage.

Results. This study offers an approach for implementing and validating a comprehensive set of cyber security measures, emphasising continuous testing and proactive updates. The cyber resilience metrics framework makes compliance in the evolving cyber security landscape mandatory using a reliability assessment based on Cronbach's alpha, which measures internal consistency reliability and the credibility of the item set. Frameworks confirm a significant correlation observed in the process of resolving cyber incidents, which means that the more accurate the information acquisition (based on metrics data), the less time is required to resolve the overall incident. Expert validation confirmed that these metrics promote compliance, competitiveness, and effective risk mitigation within a cost-effective framework. The cyber security exercise was conducted in five stages. Cyber simulation exercises and analytical hierarchy processes (AHP) are interconnected as they use a hands-on approach to the hierarchical analysis of cyber security requirements as critical elements.

Conclusions. This study identified key areas of cyber resilience based on the protection of critical infrastructure and the financial sector, using both regular testing of business continuity plans and assessments of cyber capabilities. Experimental studies adopt quantitative and qualitative data to create reliable metrics and frameworks for enhancing SMEs' cyber resilience. Thus, using the optimal cyber resilience metric framework and experiment, cyber resilience metrics can help identify organisational weaknesses in decision-making and resolve cyber incidents.

Keywords: resilience, metrics, cyber security, experiment, risk management.

e-ISSN 2786-8958
ISSN-L 2616-7107

1. Introduction.

Cyber resilience and cyber security are becoming integral elements in managing critical processes for national security as well as part of business strategy and economic sustainability (World Economic Forum, 2021). All the information exchange processes provided by digital technologies (virtual environments, cloud computing, and smart devices) are vulnerable to cyberattacks.

Researchers concluded that small and medium enterprises (SMEs) need more knowledge, competencies, awareness, and resources to obtain a data-based assessment of cyber resilience and related cyber capabilities. This research aims to study the applicability of cyber resilience metrics in solving cyber incidents and to develop an optimal cyber resilience metric framework.

The creation of the framework is based on harmonised elements of cyber security control maturity, process performance, and performance indicators, which form an optimal set to obtain a quantitative assessment of the current situation. "Optimal" in this study means that a framework (KK framework) measurement meets three criteria (high impact on the risk portfolio, low internal implementation costs, and easy maintenance) and corresponds to the experts' six functional areas of cyber resilience categories. Exemplary metrics that track risk identification, mitigation, and management accurately measure an organisation's readiness to protect critical services. Crisis simulations demonstrate the value of these frameworks, showing how metric-driven approaches support goal-oriented responses to incidents.

Additional metrics focused on strengthening business continuity further enforced operational stability while consolidating long-term resilience. In a competitive landscape of sustaining business continuity, it is key for organisations to operate both during and after disruptions. Such organisations require preliminary strategic preparation amid security breaches to uphold their critical functions. The metrics mentioned above are accumulated in a business continuity plan (BCP), which organisations use as tools for risk management, data, and system recovery.

2. Literature review.

Cyber resilience as a separate concept and category of research in the scientific literature has been found since 2015 (Björck et al., 2015). This highlights that this is not a recent development in discussion priority but rather something overlooked. Whereas similar concepts (cyber maturity) are characterised by the ability to withstand, for example, the "ability to anticipate, endure, recover and adapt to adverse conditions, stop attacks or incidents in information systems that use or associated with digital resources" (NIST, 2020). However, the term" ability to withstand "is used in social sciences", and formulates a dynamic process (Lythar et al., 2003) or including risk descriptions much earlier (Garmezy, 1990; Masten et al., 1990; Rutter, 1990).

Cyber resilience is measurable, and in the EU Directive on the resilience of critical units (European Parliament, 2022a, 2022b, 2022c), the concept of "resilience" refers to "the ability of a critical unit to avoid incidents, to protect against them, to respond to them, to resist them, to reduce or absorb them, adapt and overcome them", and there are stages of incident on the life cycle. The usability of cyber resilience metrics is depicted by Ukrainian research, which indicates dependency on the following three elements: the amount of business process functionality in the information system, the level of information resource classification (limited availability), and the security goals and priorities set in the company's security policies (Yevseiev et al., 2022).

The stakeholders' awareness level in cyber security management is closely related to their ability to determine meaningful performance indicators (Cano, 2019). Even board members do not recognise the significance of cyber security risks. At the same time, the annual threat reports of research organisations have confirmed it as leading in terms of cyber risk in the world rankings since 2017 (Allianz Commercial, 2019; Mitre & Lloyd, 2018). Multiple studies indicate that most small and medium-sized enterprises (SMEs) fail to implement adequate cybersecurity measures for continuously monitoring cyber risks, vulnerabilities, and threats (Erdogan et al., 2023).

This shortfall is primarily attributed to a limited understanding of cybersecurity skills, encompassing knowledge, abilities, and competencies (Cano, 2023).

Therefore, opportunistic cyberattacks have been identified as the most pressing to SMEs, with regulatory compliance emerging as the primary driver for adopting digital security solutions within the sector (Wilson et al., 2024). Fundamental security controls are essential, as are the ability to choose, decide, and adjust security solutions to unexpected attacks and strengthen cyber resilience (Dunn Cavelty et al., 2023).

3. Methodology.

Qualitative and quantitative research designs and methods were integrated for data collection and analysis to ensure a holistic approach to the framework-creation process. These qualitative methods (observations, expert interviews, and qualitative data analysis) were used to understand better specific research topics, motivations, factors, and element interconnections (Creswell & Poth, 2018; Patton, 2015). The research procedures were combined with quantitative data analysis. Thus, statistical analysis provides numerical insights into the prevalence and relationships of the (cyber security domain) phenomena (Babbie, 2017; Fowler, 2014).

After preparing the transcript protocols, pilot interviews were conducted to test the in-depth interview questionnaire and focus group discussion material. Qualitative data were then gathered, encoded, and normalised. Subsequently, the quantitative data were processed, including correlation and cluster analyses. Therefore, only a small subset of cyber security controls is directly attributable to cyber resilience. The study also outlines three distinct phases of the cyber incident lifecycle – before, during, and after an incident – to structure the measurements of cyber resilience across different stages of decision-making in incident response and post-incident evaluation.

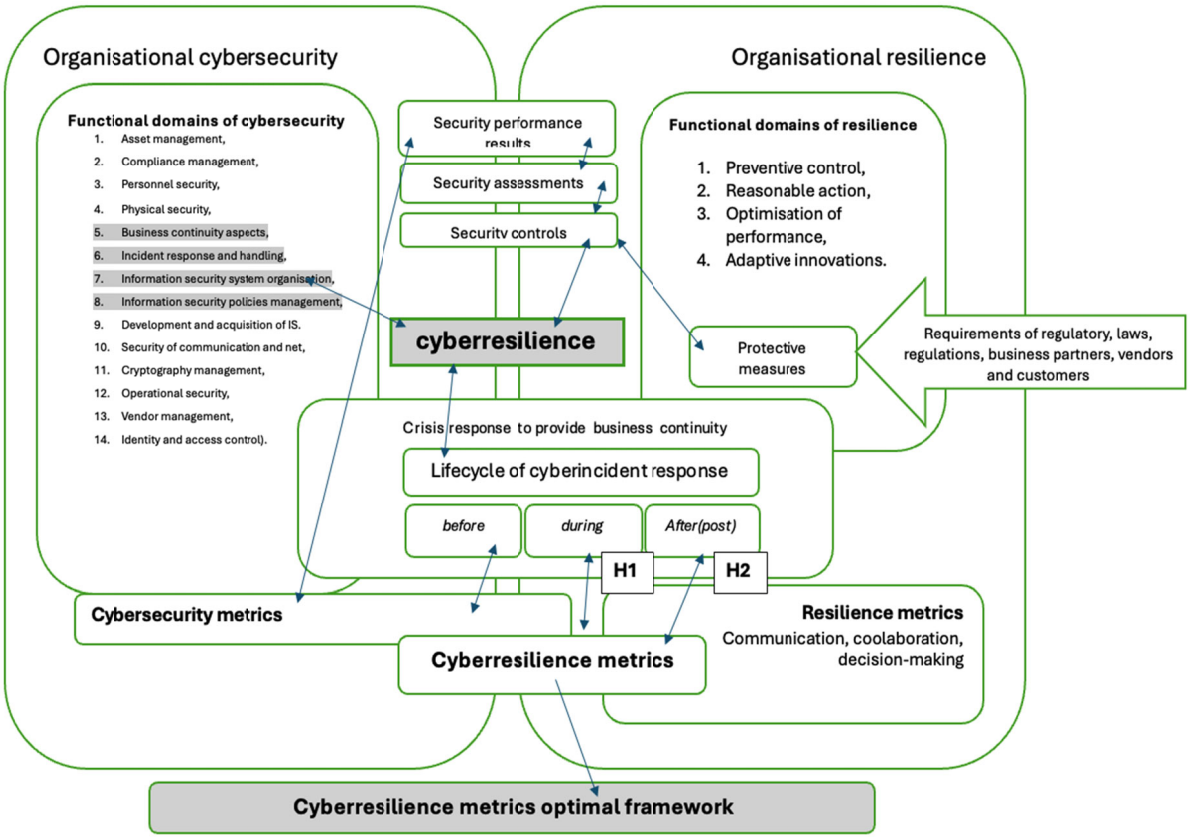


Fig. 1. The theoretical model of the framework.

Source: compiled by the author.

e-ISSN 2786-8958
ISSN-L 2616-7107

A theoretical model (Figure 1) shows the data triangulation path, consisting of literature, standard reviews, and result integration (set of criteria) to create and design a cyber security and cyber skills (KK) framework pilot for expert validation using the analytic hierarchy process method. In addition, it simulates business continuity. On the right side, this model includes four functional areas of the organisation's resilience: preventive control, reasonable action, performance optimisation, and adaptive innovation. These functional areas strengthen the components' resilience in the organisation's characterises. On the left side, 14 functional domains are distinguished by the cyber security organisation, although only four are linked to cyber resilience.

The external requirements in the model include protective measures correlated with regulatory enactments, standard requirements, and business and regulatory requirements. Usually, compliance requirements in an organisation's ecosystem are integrated with security controls. Thus, security controls include classification, evaluation, and performance indicators. The post-incident analysis phase is crucial for the assessment of the results. It helps to respond to the organisation's essential elements of resilience and cyber-skills – whether everything is done to prevent the incident from happening again – and identifies the weaknesses of cyber resilience functional domains.

The optimal set of metric framework measurements is based on the results of the quasi-experiment in the second (H1) and third lifecycle phases (H2) of the cyber-incident response. At the end of the research, the principal results were formulated, and proposals for their implementation were made.

4. Results.

4.1. Expert interviews.

The expert interview aimed to perform qualitative and quantitative cyber security metric list assessment. Based on the experts' recommendations, the interview questions, their volume, and the type of outline were adjusted by transforming them into a structured questionnaire with answers to select the experts appropriately.

After obtaining the questionnaire results, 11 experts were selected, and their characteristics are summarised below. A summary of their backgrounds revealed that 50% of the experts operate within the European Union, 30% work globally, and 20% are based in Latvia.

Additionally, 40% were risk and compliance executives, 40% served as security advisors and analysts, and 20% held IT management positions. The minimum criteria for experts' acceptance were as follows: primary cyber security control was introduced in the existing company, and the maturity of the organisation's cyber security maturity process is approaching 2nd level (67% of answers confirm the 3rd level); the individual had practical experience in implementing a security measurement program, and their professional experience was evaluated with an independent professional certificate (for example, CISA, CISM, and CRisk) and diverse backgrounds. Fourteen participants participated in the expert selection survey, 11 of whom met the criteria. Expert interviews were organised until the thematic data saturation point (i.e., during 7-8 interviews). The thematic data saturation was calculated according to the criteria described by Guest et al. (2020).

4.2. Analysis of the analytic hierarchy process for cyber security metrics to ensure confidence in the data.

AHP is a distinct method that provides strong results and has been recognised in several studies, including Mardani et al. (2015) case studies. Many criteria evaluate the approach used in cases of complex decision-making.

As a result, decision-makers could consider and assess contradictory goals and alternatives, primarily if one of the criteria is related to risks modelling uncertainty or sensitivity analysis. It is a quantitative data processing procedure (the weight and value of all criteria) that includes expert assessment consensus as an additional criterion. Industry security experts evaluated security controls based on three primary criteria: Impact on Risk Portfolio, Internal Cost of the Company, and Level of Maintenance Competencies. The results are summarised in Table 1.

After processing the interview results, experts highlighted metrics in the incident response category that influence the organisations' overall security posture and pointed out others related to crucial organisation asset identification, classification, and monitoring metrics. Reliability assessment based on Cronbach's alpha measures the internal consistency reliability and assesses the credibility of the item set. The dataset was prepared through cleaning and normalisation to analyse the cyber-resilience metrics. The expert evaluations were converted to a Likert scale using online calculation tools. The Cronbach's alpha results indicated acceptable levels of variation in internal consistency among the measurements.

Table 1. The measurement criterion's summary.

Criterion	Measurement	Value
Impact on Risk Portfolio	M7: Third-party resources identified, monitored, controlled, and supported.	High
	M8: Incidents recorded as non-compliance identified and notified.	High
	M11: Incidents of lost or stolen user equipment (annual cases known).	High
Internal Cost of the Company	M5: Information resources identified, responsible parties defined, and policies implemented.	Low
	M9: Incidents recorded as system breaks due to cyber-attacks identified.	Low
	M17: Company's outsourced risk rating evaluated; outsourcing providers classified.	Low
Level of Maintenance Competencies	M5: Information resources identified, responsible parties defined, and policies implemented.	Low
	M9: Incidents recorded as system breaks due to cyber-attacks identified.	Low
	M17: Company's outsourced risk rating evaluated; outsourcing providers classified.	Low

Information resources were identified, responsible parties were defined, and policies were implemented (M5), with a Cronbach's alpha of 0.65. Incidents recorded as system breaks due to cyber-attacks were identified (M9), with a Cronbach's alpha of 0.87 Measurement. It defines deliberate vulnerabilities in information systems (M16) with a Cronbach's alpha of 0.80. Overall, the alpha coefficients for the six categories in the measurement framework ranged from 0.71 to 0.87, demonstrating sufficient reliability for the framework used in this study.

This assessment helps to balance expert opinions on the importance of different measurements and metrics. The results can be arranged hierarchically using ranked weighting and priorities in the incident response process.

4.3. Cyber security exercise.

After expert evaluations, a cyber security exercise was conducted in five stages, according to researcher Vykopal et al. (2017). The accuracy of the simulated environment directly impacts implementation costs, but such exercises effectively reduce the cyber security competence gap (Furnell et al., 2017). Scenario exercises lasted 2–3 hours, involving 60 participants, 50–80% of whom were cyber specialists.

Their overall self-assessment results were considered average. Exercise organisers informed participants of the conditions and rules, adjusting them based on participant questions. Effective questioning facilitated informed, risk-based decision-making.

Participants were tasked with calculating operational risks using prepared policies and templates. The types and content of information requests during the scenarios were recorded and analysed. Post-exercise, data was coded and categorised into metrics, normalised for quantitative analysis, which included correlation and cluster analysis. A high correlation coefficient and significant P values are determined by proportionality (Figure 2), which indicates a strong relationship between variables. This correlation is crucial when assessing the significance of data and statistically testing hypotheses (Field, 2013; Hair et al., 2014).

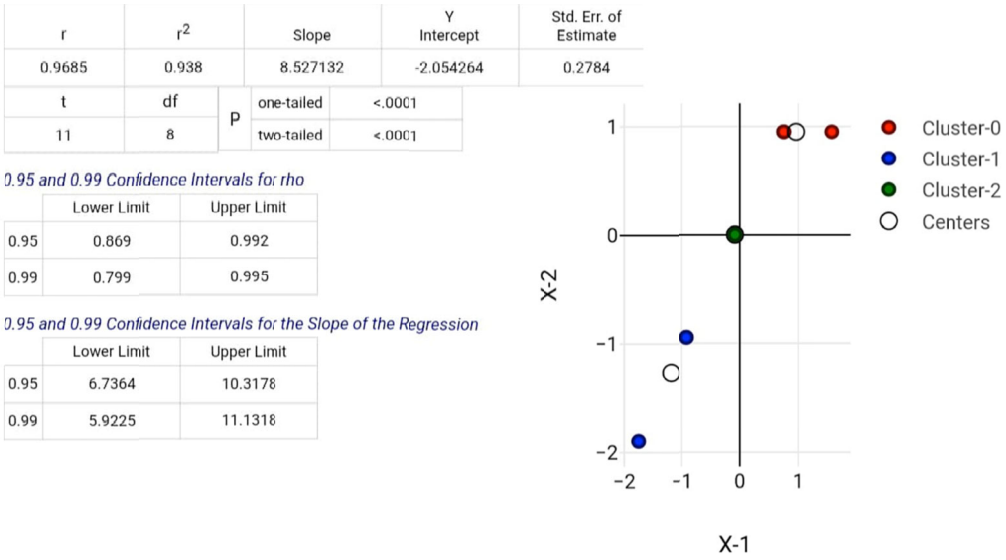
Controlled experiments are needed to test hypotheses and provide empirical evidence to prove causality in cyber security research (Shadish et al., 2002). It is possible to obtain accurate, actionable information about incident response and team performance using this method to isolate important variables (response time and information flow) (Schlette et al., 2021).

Scenario-based exercises and simulations replicate real-world conditions, enhancing the reliability of hypotheses on skills, response efficiency, and decision-making in high-stakes cyber environments (Lazar et al., 2017).

Due to the evolving nature of threats, experiments are crucial in cyber security. They facilitate assessments of team coordination and communication pathways.

Experimental studies adopt quantitative and qualitative data to create reliable metrics and frameworks for enhancing cyber resilience.

Experimental methods (Edgar & Manz, 2017; Creswell & Creswell, 2018) and cybersecurity exercise and gamification approaches (Hendrix et al., 2016; Awojana & Chou, 2019) are used to develop real-life scenarios.



r	r^2	Slope	Y Intercept	Std. Err. of Estimate
0.9685	0.938	8.527132	-2.054264	0.2784

t	df	P	one-tailed	<.0001
11	8		two-tailed	<.0001

0.95 and 0.99 Confidence Intervals for rho

	Lower Limit	Upper Limit
0.95	0.869	0.992
0.99	0.799	0.995

0.95 and 0.99 Confidence Intervals for the Slope of the Regression

	Lower Limit	Upper Limit
0.95	6.7364	10.3178
0.99	5.9225	11.1318

Fig. 2. The correlation and cluster analysis results (x1-information, x-2 time).

A significant correlation can be observed in resolving cyber incidents, which means that the more accurate the information acquisition, the less time is required to resolve the overall incident. Thus, the amount of information correlates with a particular time, as shown in the indicators in Figure 2.

Scenario-based exercises that are a part of the experimental approach are practical for developing cyber skills. Participants recognised that incident investigation and post-incident analysis identify factors and vulnerabilities that can improve the incident response lifecycle. Such analyses reveal communication shortcomings and gaps in information that hinder decision-making, a disadvantage noted during focus group discussions on security metrics.

Additionally, these insights point to potential avenues for process automation. Focus group discussions identified several security risks that are consolidated in Table 2.

Table 2. The consolidation of risk was identified after focus group discussions.

Areas for Improvement	Gaps and Needs
Post-incident analysis, details and complete information	Incident, investigating, processing, handling and reporting procedures
Actual security-related metrics and indicators	Start to implement a metrics program
Business continuity plan testing methods	Need to differ testing methods, such as table-top
Communication channels tools are missing	Need to develop crisis communication plans, guidelines
The current cyber security competencies are untested and incompetent	Proficiency in incident response
Lack of documentary basis for decision making in crisis situations	Involve C-level executives in BCP

These types of testing and auditing are meaningful in improving an organisation's cyber security maturity and ensuring business continuity during crises. Additional testing methods improve productivity and help staff maintain cyber resilience. Employee decision-making is the main focus of cyber resilience assessments, based on ongoing training in real-life scenarios that help employees understand their responsibilities and follow protocols.

Relying on a single test may fail to uncover flaws, highlighting the need for ongoing performance improvements. The KK framework enhances security controls by categorising them into functional areas, linking them to the stages of the incident lifecycle, and clarifying the tasks associated with each stage.

5. Conclusions.

Cyber resilience is a structural element in cyber security management. The aspects of cyber resilience illuminate an organisation's ability to manage crises effectively. The performance of cyber security teams is characterised by collaboration, responsiveness, and information-sharing competencies, essential soft skills elements for successful crisis management.

SMEs in the EU that provide cyber security consulting services to DORA-compliant organisations or critical infrastructure entities may face significant challenges. These challenges include staying compliant with regulations regarding mandatory cyber security requirements (e.g. DORA), maintaining cyber security competencies, managing supply chain risks, and integrating cyber security with broader risk management frameworks. To mitigate these challenges, SMEs must invest in the right assets, granular technologies, and training personnel. Thus, using the KK metric framework and experiments, cyber resilience metrics help identify organisational weaknesses in decision-making and resolve cyber incidents.

The creation of the framework is based on harmonised elements of cyber security control maturity, process performance, and performance indicators, which form an optimal set to obtain a quantitative assessment of the current situation.

Organisations must relentlessly demonstrate their ability to adapt to and recover from incidents to overcome challenging obstacles. Crises often generate innovations and alternative solutions despite resource deficits. Cyber resilience can be gradually developed, and this process should cover at least three levels: employees, processes, and technology. The classification of cyber security controls is essential for identifying, coordinating, and prioritising the implementation of protective measures. Therefore, risk levels are addressed based on asset classification and the value of informational assets.

Furthermore, this classification is necessary to ensure compliance with regulatory and legislative requirements. To implement adequate cyber security measures, it is vital to increase the awareness of cyber security metrics and their diversity and promote the diversity of utility. Various types of assessments, including cyber security control and process maturity assessments, are integral to understanding the overall level and effectiveness of cyber security management. Implementing basic cyber security measures requires many small- and medium-sized enterprises to have IT tools and additional knowledge in cyber security management. This gap resulted in their inability to identify where to invest effectively in cyber security.

Automated and continuous cyber resilience assessment offers a more accurate perspective on cyber security across functional areas. The summarised risk list is merged with the cyber security metrics program implementers. Information security managers generally require additional time, technical resources, and competencies for effective metric program implementation.

The research emphasises that organisations must prioritise developing a structured approach to cyber security through systematic assessments, practical competencies, subskill identification, and resource allocation. All procedures were conducted following ethical guidelines. Established safety standards were strictly followed throughout the study. This included informed consent, protection of participants' confidentiality, data pseudonymisation procedures, and ensuring transparency and accurate data interpretation.

REFERENCES

Allianz Commercial. (2019). Allianz Risk Barometer: Top business risks for 2019. Munich, Germany.

Awojana, T., & Chou, T. (2019, February), Overview of Learning Cybersecurity Through Game Based Systems Paper presented at 2019 CIEC, New Orleans, LA. 10.18260/3-2-370-31521

Babbie, E. (2017). The practice of social research (14th ed.). Cengage Learning.

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience – Fundamentals for a definition. In A. Rocha, A. Correia, S. Costanzo, & L. Reis (Eds.), New contributions in information systems and technologies (Vol. 353, pp. 159-166). Springer. https://doi.org/10.1007/978-3-319-16486-1_31

Cano, J. (2019). The human factor in information security. ISACA Journal, 5, 1-8.

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications, Inc.

Creswell, J.W. & Poth, C.N. (2018). Qualitative Inquiry and Research Design Choosing among Five Approaches. 4th Edition, SAGE Publications, Inc., Thousand Oaks.

Dunn Cavelty, M., Eriksen, C., & Scharte, B. (2023). Making cyber security more resilient: adding social considerations to technological fixes. Journal of Risk Research, 26(7), 801–814. https://doi.org/10.1080/13669877.2023.2208146

Edgar, T. W., & Manz, D. O. (2017). Research methods for cyber security. Syngress.

Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S., & Pickering, B. (2023). Cybersecurity awareness and capacities of SMEs. In Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP) (pp. 296–304). SciTePress. https://doi.org/10.5220/0011609600003405

European Parliament. (2022a). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cyber security across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 (NIS2). Official Journal of the European Union, L333, 80–140.

European Parliament. (2022b). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Official Journal of the European Union, L333, 27.12.2022.

European Parliament. (2022c). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, and (EU) No 909/2014 (DORA). Official Journal of the European Union, L333, 1–79.

Field, A. (2013). Discovering statistics using IBM SPSS statistics (4th ed.). SAGE Publications.

Fowler, F. J. (2014). Survey Research Method (5th ed.). Centre for Survey Research, University of Massachusetts.

Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. Computer Fraud & Security, 2017(2), 5–10. https://doi.org/10.1016/s1361-3723(17)30013-1

Garmezy, N. (1990). Closing note: Reflections on the future. In J. Rolf, A. Masten, D. Cicchetti, K. Nuechterlein, & S. Weintraub (Eds.), Risk and protective factors in the development of psychopathology (pp. 527–534). Cambridge University Press.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2014). Multivariate data analysis (7th ed.). Pearson.

Hendrix, M., Al-Sherbaz, A., & Bloom, V. (2016). Game based cyber security training: Are serious games suitable for cyber security training? International Journal of Serious Games, 3(1), 53–61. https://doi.org/10.17083/ijsg.v3i1.107

Jeimy, J., & Cano, M. (2023). FLEXI - A conceptual model for enterprise cyber resilience. Procedia Computer Science, 219, 11–19. https://doi.org/10.1016/j.procs.2023.01.258

Lazar, J., Feng, J. H., & Hochheiser, H. (2017). Research methods in human-computer interaction. Morgan Kaufmann.

Mardani, A., Zavadskas, E. K., Khalifah, Z., Jusoh, A., & Nor, K. M. (2015). Multiple criteria decision-making techniques in transportation systems: a systematic review of the state of the art literature. Transport, 31(3), 359–385. https://doi.org/10.3846/16484142.2015.1121517

MITRE. (2018). Cyber security metrics catalogue: Technical guidelines.

NIST. (2020). Cybersecurity. Retrieved from https://www.nist.gov/cybersecurity

Patton, M. (2015) Qualitative Research and Evaluation Methods. 4th Edition, Sage Publications, Thousand Oaks.

Rutter, M. (1990). Psychosocial Resilience and Protective Mechanisms. In J. Rolf, A. S. Masten, D. Cicchetti, K. H. Nuechterlein, & S. Weintraub (Eds.), Risk and Protective Factors in the Development of Psychopathology (pp. 181-214). New York: Cambridge University Press. https://doi.org/10.1017/CBO9780511752872.013

Schlette, D., Caselli, M., & Pernul, G. (2021). A comparative study on cyber threat intelligence: The security incident response perspective. IEEE Communications Surveys & Tutorials, 23(4), 2525-2556. http://dx.doi.org/10.1109/COMST.2021.3117338

Shadish, W. R., Cook, T. D., & Campbell, D. T. (2002). Experimental and quasi-experimental designs for generalized causal inference. Houghton, Mifflin and Company.

Vykopal, J., Vizvary, M., Oslejsek, R., Celeda, P., & Tovarnak, D. (2017). Lessons learned from complex hands-on defence exercises in a cyber range. 2017 IEEE Frontiers in Education Conference (FIE) (pp. 1–9). https://doi.org/10.1109/FIE.2017.8190592

Wilson, M., & McDonald, S. (2025). 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

Yevseiev, S., Milov, O., Opirskyy, I., Dunaievska, O., Huk, O., Pogorelov, V., Bondarenko, K., Zviertseva, N., Melenti, Y., & Tomashevsky, B. (2022). Development of a concept for cybersecurity metrics classification. Eastern-European Journal of Enterprise Technologies, 4(4 (118)), 6–18. https://doi.org/10.15587/1729-4061.2022.263416