Integrating Business Continuity Management, Cybersecurity, and Organisational Resilience Against Cyber Disruptions

ILKKA TIKANMÄKI, HARRI RUOSLAHTI
ResLab, Security and Risk Management
Laurea University of Applied Sciences
Vanha maantie 9 FI-02650 Espoo
FINLAND

Abstract: - This study examines the integration of business continuity management (BCM), cybersecurity and organizational resilience, with an emphasis on human factors. The study brings together key findings that support the development of organizational resilience. The study compiles the findings of 13 peer-reviewed publications resulting from the efforts of tasks 8.2 of the ECHO and 3.2 of the DYNAMO projects. The study highlights gaps in current commercial tools for business continuity management, cyber threat intelligence (CTI) and risk management (RM). The DYNAMO platform is an AI-driven solution that enables cybersecurity resilience through simulation-based training and decision support systems.
The articles cover topics such as combining business continuity management principles to build dynamic resilience, the role of communication in organizational resilience and the role of human factors in cybersecurity. The study examines the implementation of guidelines to improve cybersecurity, the use of open-source intelligence (OSINT) in the financial sector, and the impact of the EU AI law on cybersecurity training.
The analysis highlights the importance of integrating continuity planning and risk management into organizational culture, supported by effective communication, continuous learning, and the adoption of recognized standards. The results provide practical advice for organizations seeking to improve their preparedness for hybrid threats and disruptions, and suggest further research directions for resilience assessment, AI integration, and cross-sector standardization.

Key-Words: - Business Continuity Management (BCM), Cybersecurity, Organizational Resilience, Human Factors, Risk Management, Cyber Threat Intelligence (CTI)

Received: July 14, 2025. Revised: March 19, 2026. Accepted: April 11, 2025. Published: June 25, 2026.

1 Introduction

Digitalization, interdependence, and cyber-physical threats create complex disruptions for organizations. The established practices include BCM, cybersecurity, and risk management. The fact that they are implemented separately often leads to gaps in situational awareness, human-factor integration, and cross-functional decision-making. The existing BCM, CTI, and risk assessment tools do not provide support for dynamic resilience or coordinated responses to disruptions. The ECHO and DYNAMO projects address these challenges by developing integrated, human-centric approaches. The publications from these projects provide the empirical basis for this research. The research problem is the lack of a unified understanding of how to operationalize BCM, cybersecurity, and organizational resilience. The study examines whether such integration, which is supported by human factors, can enhance organizations' preparedness for disruptions.

This study presents research findings published in academic journals and conferences on human factors in business continuity management (BCM), cybersecurity, and organizational resilience. The research draws on the publications produced by two major European projects: the European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations (ECHO) and the Dynamic Resilience Assessment Method, including a combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors (DYNAMO) [1], [2]. The articles are a combination of insights from ECHO and DYNAMO research activities and previous publications by experts in the field on how to enable modern organizations to strengthen their resilience to disruptions, effectively manage cyber threats, and ensure critical functions remain operational.

The shared commitment of the projects to innovation, excellence, and human-centered approaches can be seen in these works, which have been published in conference proceedings and peer-

reviewed scientific journals. The ECHO project aimed to bring together European cybersecurity efforts, while DYNAMO aimed to integrate AI into cybersecurity training and decision-making to safeguard critical infrastructure. The DYNAMO project aims to enhance recovery and resilience against cyber threats through AI-driven simulations and decision-making tools. Project ECHO work is partially furthered in DYNAMO, as some project partners and researchers have collaborated on both projects, and the ECHO Early Warning System (E-EWS) is a component of the DYNAMO platform.

2.1 Objectives and research questions

The research is based on thirteen case studies that deepen our understanding of human factors in cybersecurity. These cases contribute to the growing body of knowledge that helps create more resilient and responsive organizations. The thirteen case studies combine into a body of knowledge that enhances project understanding of human factors in cybersecurity. The research question of the study is:

Can business continuity management, cybersecurity, and organizational resilience be integrated to improve organizational readiness against disruptions?

The core themes of the research are reflected in this question, which integrates business continuity management, cybersecurity, and resilience, emphasizes human factors, and explores the practical outcomes of organizational readiness.

The structure of this paper is as follows: Chapter II provides a relevant literature review, Chapter III describes the research methodology, Chapter IV presents the study's findings, and Chapter V concludes the research with recommendations.

2 Literature review

The research content can be analyzed and presented in a structured manner, with the following themes highlighting key focus areas and their connections.

2.1 Business Continuity Management (BCM)

According to ISO 22301, the definition of the BCM is a system of interrelated elements that organizations use to establish, implement, operate, monitor, review, maintain, and enhance their business continuity capabilities [3]. BCM systems aim to provide guidance and analytical frameworks for risk assessment, management, and operational maintenance during disruptions. Current BCM practices have a common structure for formal planning processes and risk assessment activities.[4]. BCM is a comprehensive management process that recognizes threats and their consequences and creates a foundation for an organization's resilience [5]. The process consists of steps like planning, absorbing, recovery, and adaptation, which together enhance an organization's ability to respond to and recover from disruptions [6].

BCM was developed several years ago and is an evolution of the company's disaster recovery approach. Although its origins lie in information security (IS), it has arguably evolved significantly since then [5]. The BCM approach aims to give a framework for comprehending how value is created and maintained in an organization and establish a direct connection between the dependencies or vulnerabilities associated with value creation. The implementation of this approach involves a holistic and multidisciplinary approach [5]. A cybersecurity resilience framework is crucial for businesses in today's digital environment. The framework enhances cybersecurity defenses and contributes to an overall risk management strategy, guaranteeing business continuity [7].

2.2 Resilience

According to the National Academy of Sciences (NAS), resilience is "the ability to prepare for, plan for, survive, recover from, and adapt more successfully to adverse events." [8]. Dynamic resilience is a term used to describe an organization's ability to respond and recover quickly from adverse events [9]. The new normal demands collaboration on social networks, continuous communication, and adaptability [10]. The resilience management framework relies on risk analysis as a key component. To determine the expected loss of critical functionality, risk analysis is based on the identification of threats, vulnerabilities, and consequences of adverse events [11]. Figure 1 presents the resilience management framework that includes risk analysis.

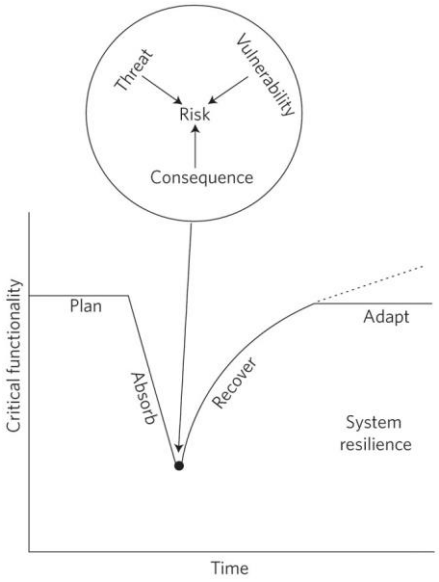

Fig.1. A resilience management framework [11].

The interpretation of system risk is that of the overall degradation of critical functionality, and system resilience is linked to the slope of the absorption curve and the shape of the recovery curve. This demonstrates the temporal impact of an adverse event on the system. Highly resilient systems could adjust to improve the system's functionality compared to its original performance. The dotted line indicates that this improves the system's ability to withstand future adverse events [11]. Implementing resilience strategies that enable systems to remain operational and recover effectively from disruptions is essential, as societies and economies are still susceptible to systemic disruptions and rapidly changing conditions [12]. Resilience is a valuable alternative method for analyzing complex systems and systemic risks that are hard to analyze using traditional risk assessment methods. A resilience-based approach is beneficial for many modern systems [13].

Collaborative and multidisciplinary approaches are necessary for comprehensive risk and resilience management strategies. To fully comprehend the range of factors that affect an organization down to the system level, they combine social, economic, and technical perspectives. Maintaining acceptable critical infrastructure performance requires a combination of social and systems engineering approaches to support multi-organizational decision-making. [14]. Organizations can anticipate trends, seize opportunities, and mitigate risks by utilizing their adaptability, organizational learning, and dynamic capabilities. Continuous learning leads to innovation and flexibility, and organizations benefit from adaptability and dynamic capabilities to adapt strategies and integrate competencies, improving resilience and driving systematic development. [10].

2.3 Cybersecurity

Cybersecurity is categorized as an interdisciplinary field. Scientific research is not easily applicable to cybersecurity because it is not a clearly defined academic field. Cybersecurity is a mix of technical, behavioral, and cultural disciplines. The rapid evolution of threats, the difficulty of conducting controlled experiments, and the pace of technological change and innovation make scientific research complicated. [15]. The definition of cybersecurity is not internationally accepted or standardized, and there is no clear identification of its development and application area. Cyberattacks are a threat in the new reality where digital transformation is a major factor. The implementation of cybersecurity measures is necessary due to the potential for data breaches caused by digital threats [16]. The importance of cybersecurity lies in the sharing of information and trust. Due to the increase in cybersecurity incidents, it is necessary to protect against a variety of threats, such as cyberattacks, dynamic and evolving advanced persistent threats, privacy breaches, power outages, and serious human errors that occur because of inadequate training [16].

The growing importance of digital transformation has made cybersecurity a crucial research area. The challenges identified are mainly due to the lack of funding, a restricted skilled workforce, and a lack of cybersecurity policy or regulatory guidance [17]. Research on cybersecurity issues, which are considered multidisciplinary, has increased due to the increased use of technology [18]. There is a persistent need to enhance understanding of the specific nature of organizational cybersecurity, the cybersecurity skills necessary for it, and the relevant methods for acquiring those skills [18].

Human factors in cyber security, e.g., training, cognitive biases, organizational culture, encompass environmental, organizational, and job-related factors, as well as human and individual characteristics, that impact work behavior in ways that can impact health and safety [19]. The study of human factors focuses on the interaction between humans and system components [20]. Human factors in cybersecurity are examined by researchers from different fields who focus on highlighting several perspectives: organizational needs, challenges, and skill gaps [18]. Successful cybersecurity leadership requires consideration of human factors. Senior management is crucial in this area, and people should always be the focal point of daily operations. [21]. The findings of [22] indicate the necessity of establishing formal training and learning standards

that empower organizations to tackle the human factors of cybersecurity and critically mitigate cyber risks. IT systems should be able to detect phishing emails and other social engineering attacks, while, e.g. healthcare professionals should have the ability to identify social engineering [22].

3 Methodology

Systematic reading of materials, observation, interviews, surveys, and reporting of their results are the fundamental components of a case study research process [23], [24]. The case study approach offers a distinct method for observing any natural phenomenon that occurs in a specific set of data [25]. Case studies are centered around examining either a specific number of individuals or an area as research subjects [26]. The researcher can create a comprehensive picture by highlighting relevant aspects while examining real-life phenomena through detailed contextual analysis of a limited number of events or circumstances and their relationships [27].

Data from specific contexts were provided to the project consortium researchers using a case study approach. Research efforts involved the writing of a qualitative synthesis, of 13 previously published project outputs. These were considered as case studies and a cross-case analysis provided knowledge on the human factors of cybersecurity with an emphasis on the healthcare, maritime, and energy sectors. These cases were presented as peer-reviewed research articles in academic conferences and journals. The following table features 13 articles on business continuity management (BCM), cybersecurity, human factors and organizational resilience written for the DYNAMO and ECHO project tasks.

To convey narrative analysis of text and interview materials, the analysis utilized qualitative approaches. Researchers aimed to combine relevant aspects to reveal the bigger picture and provide a thorough understanding of the research context in T3.2. Since all thirteen publications originate from the same research ecosystem of projects ECHO and DYNAMO), there is a risk of selection bias.

Table 1. Related articles written in the DYNAMO and ECHO projects.

#	Authors	Publication title	Publication channel
1	Hytönen & Ruoslahti (2024) [28]	Business Continuity Management – Building Block of Dynamic Resilience	Journal: Critical Information Infrastructures Security Lecture Notes in Computer Science
2	Hytönen & Ruoslahti (2023) [29]	A Lens to Examine Communication Through Business Continuity Management	Book chapter: Public Relations and Sustainability
3	Ruoslahti & Hytönen (2024) [30]	Academic publications create sustainable knowledge in funded projects	Book chapter: Public Relations and Sustainability
4	Savolainen, McCarthy, Neville & Ruoslahti (2024) [31]	Business Continuity Management of Critical Infrastructures from the Cybersecurity Perspective	Conference: IEEE Global Engineering Education Conference
5	Tikanmäki & Ruoslahti (2024a) [32]	Enhancing Security Education: A Comprehensive Analysis of Virtualized Learning Approaches in the Study of Hybrid Threats	Conference: IEEE Global Engineering Education Conference
6	Heinonen & Ruoslahti (2024) [33]	Measuring Societal Impacts of Cybersecurity	Conference: European Conference on Cyber Warfare and Security
7	Ruoslahti, Hytönen & Sanchez (2024) [34]	Business Model Canvas and Competition to Understand Exploitation of Cybersecurity Project Results	Conference: European Conference on Cyber Warfare and Security
8	Ruoslahti & Tikanmäki (2024) [35]	The Social Domain: Resilience of Information-Sharing	Conference: European Conference on Cyber Warfare and Security
9	Rajamäki & Tiitta (2024) [36]	Implementation of OSINT for Improving an International Finance Sector Organization's Cybersecurity	Conference: International Conference on Cyber Warfare and Security
10	Tikanmäki, Savolainen & Ruoslahti (2024) [37]	The Role of Standards in Enhancing Cybersecurity and Business Continuity Management for Organizations	Journal: Information & Security: An International Journal

11	Tikanmäki & Ruoslahti (2024b) [38]	Human Factors Make or Break Cybersecurity!	Journal: Information & Security: An International Journal
12	Rajamäki, Savolainen & Tikanmäki (2025) [39]	The Effect of EU's Artificial Intelligence Act on Cyber Security Training	Journal: Futureproofing Engineering Education for Global Responsibility,
13	Tikanmäki & Ruoslahti (2024c) [40]	Insights on Human Factors Enhancing Cybersecurity	Journal: Information & Security: An International Journal

These articles serve as the data for this study. Each article focuses on a specific scenario or organizational environment. Examples of case study topics include cybersecurity training and awareness, phishing resilience and employee behavior at a national energy company, organizational learning from cyber incidents in healthcare IT, cross-sector collaboration to share cyber threat information, and human error. The dissemination of these case studies as peer-reviewed research articles at academic conferences and journals contributed to the knowledge base at the intersection of human factors and cybersecurity.

4 Results

Combined, the sample studies discuss the importance of a comprehensive approach to resilience that incorporates technological, human, and organizational factors. Topics covered include combining business continuity principles to create dynamic resilience, the importance of communication in organizational resilience, the effect of academic publications on project sustainability, and the significance of human factors in cybersecurity. Sample articles also examine how standards can improve cybersecurity, how open-source intelligence (OSINT) can be utilized in financial cybersecurity, and how the AI law of the European Union affects cybersecurity education.

Combining diverse perspectives can help summarize the use of practical frameworks, innovative methodologies, and critical challenges. This can help to present a comprehensive view of current trends and future directions in these essential areas. Sample research emphasizes the significance of incorporating continuity planning and risk management into organizational culture. Active participation at all levels of the organization is necessary to guarantee readiness and adaptability in the face of changing threats.

The collection of articles in Table 2 examines the characteristics of business continuity management (BCM), cybersecurity, human factors, and resilience in both organizational and educational contexts. The table presents the main themes, methodology, and key focus areas.

Table 2. The main themes, methodology and key focus of the articles.

Article #	**Theme**	**Methodology**	**Key focus**
1	BCM & resilience	Qualitative interviews	Adaptive BCM practices
2	Communication in BCM	Framework analysis	Communication strategies
3	Project sustainability	Participatory action research	Academic publishing
4	Cybersecurity & BCM	Literature review	Human factors & AI
5	Hybrid threats education	Mixed methods	Virtualized learning
6	Cybersecurity impact	Surveys & statistical analysis	SIA Toolkit
7	Market dynamics	Action research	BMC&C framework
8	Social networks	Risk matrix	Network resilience traits
9	Threat intelligence	Design Science Research	OSINT process
10	Standards & regulation	Comparative analysis	ISO/NIST frameworks
11	Human vulnerabilities	Theoretical analysis	Holistic approach
12	AI regulation & education	Policy analysis	Curriculum adaptation
13	ECHO project insights	Case study	Training & awareness

BCM as Dynamic Resilience explores how BCM helps organizations adapt to disruptions through continuous planning and communication, based on interviews with Finnish experts. Communication in BCM introduces a resilience matrix to highlight communication's role across BCM phases, stressing its importance in decision-making and situational awareness. Academic Publishing in Projects argues that early academic publishing improves project

outcomes and sustainability, using co-creative writing and participatory research. Cybersecurity in Critical Infrastructure BCM proposes a new BCM framework integrating AI and human factors, emphasizing continuous learning for resilience in sectors like energy and healthcare. Virtual Learning for Hybrid Threats evaluates a hybrid threat course using virtual modules, showing improved student understanding and critical thinking through structured education. Societal Impact of Cybersecurity uses statistical tools to assess how cybersecurity affects society, highlighting the importance of European solutions and communication skills.

Business Model Canvas & Competition enhances the traditional BMC by adding a competition block, helping organizations better understand market positioning in cybersecurity. Resilience in Info-Sharing Networks identifies traits like trust and leadership that strengthen network resilience, with practical tools developed in the DYNAMO project. OSINT for Cybersecurity details a structured OSINT process for threat intelligence in finance, suggesting AI integration for future improvements. Standards in Cybersecurity & BCM reviews ISO and NIST standards, noting their potential but also the lack of practical implementation evidence, calling for further research. Human Factors in Cybersecurity discusses how traits like fear and trust affect cybersecurity, advocating for a holistic approach that includes legal, ethical, and organizational aspects. EU AI Act & Cybersecurity Education analyses how the AI Act impacts cybersecurity training, recommending curriculum updates to address legal and technical challenges. Human Factors in ECHO Project highlights training and awareness as key to cybersecurity, showing how human factors influence resilience and organizational culture.

The table below displays the findings of a review of the shortcomings found in commercial tools for business continuity management (BCM), cyber threat intelligence (CTI), and risk management (RM). In the following table, the Theme refers to the main topic or focus area of the article (e.g. business continuity management, communications, artificial intelligence training). Key insight refers to the core findings or contribution of the research, and Practical implication explains how the insight can be applied in real-world organizational or strategic contexts.

Table 3. Key conclusions from reviewed articles.

Theme	**Key insight**	**Practical implication**
Dynamic Resilience through BCM	Effective BCM practices, characterized by continuous risk assessment, regular exercises, and open communication, are essential for building dynamic resilience	Organizations must embed BCM into their culture to ensure all levels are involved in continuity planning and risk management
Communication as a Pillar of Resilience	Communication plays a pivotal role in maintaining situational awareness, supporting decision-making, and fostering a culture of resilience	The modified Resilience Matrix offers a valuable framework for integrating communication management with resilience planning
Sustainability through Academic Publications	Early focus on academic publications in funded projects can enhance knowledge creation, project sustainability, and academic visibility	Early integration of structured academic publishing strategies to maximize project lifecycle impact is recommended for organizations and consortia to facilitate knowledge dissemination, stakeholder engagement, and long-term impact.
Cybersecurity and Human Factors	Integrating human factors into cybersecurity and BCM frameworks is crucial for improving the resilience of critical infrastructures	Continuous training and adaptation are necessary to address human vulnerabilities and enhance threat detection and response.
Educational Innovations in Security	Virtualized learning approaches and structured modules in security education can significantly enhance students' understanding and preparedness for hybrid threats	Feedback from such programs can inform future educational initiatives.
Measuring Societal Impacts	Tools like the Societal Impact Assessment Toolkit are practical for evaluating the societal impact of cybersecurity efforts	Continuous development and standardization of such tools are needed to improve their effectiveness.
Business Model Adaptations	Incorporating competition into Business Model Canvas provides a more comprehensive framework for analyzing business models,	This approach aids in strategic planning and market positioning.

	particularly in the cybersecurity sector	
Resilience of Information-Sharing Networks	Understanding and implementing key resilience attributes can significantly improve the ability of organizations to withstand disruptions	Collaborative networks must prioritize clear purpose, defined roles, and open communication.
Role of Standards in Cybersecurity	Standards like ISO 22301, ISO/IEC 27001, and the NIST Cybersecurity Framework are valuable for enhancing cyber resilience and business continuity	Practical experiences and newer regulations need further exploration to maximize their benefits.
Impact of AI on Cybersecurity Training	The EU's AI Act necessitates adaptations in cybersecurity curricula to address emerging challenges in AI-driven technologies	Continuous learning and updates are essential for preparing cybersecurity professionals.

Table 3 includes the study's findings and suggested solutions for capabilities for resilience, operational integration, learning and adaptation, and overall cybersecurity effectiveness. Thirteen academic articles have covered the subject, and the results that were discovered to address the shortcomings are presented in the right column.

The reviewed studies point out the significance of combining technological, human, and organizational facets for resilience. Findings highlight that BCM, cybersecurity practices, and organizational resilience should be seen as interconnected parts within a unified resilience framework. In summary resilience becomes fostered with ongoing training/education across organizations to align technical systems, human capacities, and organizational approaches.

5 Discussion and Conclusions

The findings highlight the advantages of integrating business continuity management, cybersecurity, and organizational resilience. However, there are visible limitations that should be considered.

Firstly, outcomes are based publications from the just two connected projects, ECHO and DYNAMO, which limits the generalizability to contexts beyond comparable European research environments. This suggests that the recognized integration advantages may be, in part, affected by the shared assumptions, frameworks, and research goals of the projects. Secondly, real-world challenges, such as silos, competing goals, and resource constraints, hinder the adoption of comprehensive resilience methods. Thirdly, there are underlying conflicts in the heightened use of AI-driven tools and standardized methodologies. These tensions reveal the necessity for a balanced method that combines technological progress with vigilant human oversight.

The results of a comparison of commercial business capability management (BCM), cyber threat intelligence (CTI), and risk management (RM) tools revealed several limitations. The solution of the DYNAMO underlying principles was compared to these limitations to address them by improving resilience, operational integration, learning, adaptation, and cybersecurity effectiveness. This study offers an overview of recent research and advancements in business continuity management (BCM), cybersecurity, and organizational resilience from thirteen academic articles. Results highlight the importance of integrating robust BCM practices, effective communication strategies, and human-centric approaches into organizational frameworks to enhance resilience against a variety of disruptions (Figure 2).

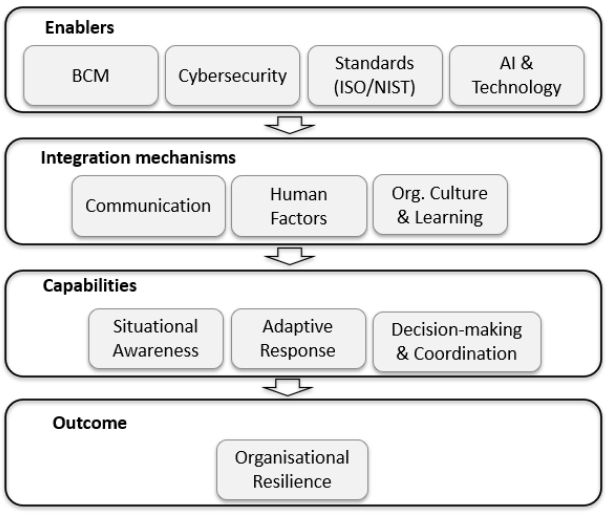

Fig. 2. Conceptual Model of Integrated Organisational Resilience

Figure 2 is a visual summary of the key themes and relationships and essential areas of study: business continuity management, communication, human factors, and AI and technology. Communication, training, leadership, organizational culture, standards adoption, and continuous learning appear throughout the dataset as recurring themes and practical implications.

This model demonstrates how the elements of business continuity management, cybersecurity, standards, and artificial intelligence technologies serve as enablers. Communication, human factors, and organizational culture facilitate their integration and promote essential organizational functions, situational awareness, adaptive responses, and coordinated decision-making that jointly enhance organizational resilience. Continuous learning is a key component in reinforcing resilience through feedback mechanisms.

Business continuity management incorporates both continuity planning and risk management. Cybersecurity focuses on addressing vulnerabilities and cyber threats. Human factors foster a strong culture of resilience. Training and continuous improvement are key aspects of learning and adaptation. All the above are connected by enhancing organizational resilience, which is a crucial factor.

5.1 Practical Implications

This paper synthesizes findings from thirteen peer-reviewed publications into a coherent framework for organizational resilience. The practical impact of each category indicates how the findings can be utilized in real-life situations. Organizations seeking to strengthen their resilience and cybersecurity posture can benefit from the practical insights provided by this study. Organizations need to move beyond compliance-based approaches and integrate business continuity planning into their organizational culture. The focus is on regular training, scenario-based exercises, and leadership engagement at all levels. Effective communication is crucial during disruptions, which is why it is important to improve communication strategies. Frameworks, such as a modified resilience matrix, are a way for organizations to align communication planning with resilience goals and ensure clarity, responsiveness, and coordination. However, such integration efforts may encounter organizational silos, resource constraints, governance conflicts, cultural resistance, and regulatory complexity.

AI-based simulations and decision support tools can enhance preparedness and responsiveness in cyber resilience. Critical industries should consider integrating AI into training and threat analysis. Improving security training programs necessitates the inclusion of virtual learning environments and structured modules that reflect real-world hybrid threats. Content can be adapted to changing needs and learner profiles with the help of feedback mechanisms. Leveraging standards and assessment tools: Adopting recognized standards (e.g., ISO 22301, ISO/IEC 27001, NIST) and tools such as the Societal Impact Assessment Toolkit can guide organizations in assessing and improving their resilience strategies. Limitations that may be associated with AI adoption may include explainability, bias, overreliance on automation, privacy concerns, regulatory uncertainty, and the evolving requirements of the EU AI Act.

Organizations focused on cybersecurity can improve their market positioning by incorporating competitive dynamics into strategic planning using tools such as the Business Model Canvas. These practical significances support a proactive and integrated approach to crisis resilience and encourage organizations to transition from reactive risk management to dynamic, adaptive systems.

The main implication of this research centers around positive developments in academic publishing, training, and collaboration. Future research should incorporate a wider variety of empirical evidence, such as failed cases, to achieve a more balanced and critical assessment of resilience development. The ability to provide a comprehensive overview of recent advances is hindered by focusing on published articles from specific projects. All emerging trends, practices or frameworks may not be entirely covered by the study. Furthermore, the assessment of commercial tools is based on the documentation and opinions of experts, which may not reflect all actual implementations. Future study would benefit from a wider investigation of external literature on e.g. cyber resilience, organizational resilience, socio-technical cybersecurity frameworks, and resilience engineering.

Models related to cyber resilience, enterprise resilience, socio-technical systems, and organizational adaptability serve as frameworks for future research efforts, which should continue to explore these intersections to improve organizational resilience and manage disruptions effectively. Future research could also examine the interrelationships between business capability management, cybersecurity, and human factors, particularly in the context of evolving threats and technological advances. Other areas of future research include the long-term impact of communication strategies on organizational resilience and comparing studies across industries to validate the generalization of the findings.

References:

[1] DYNAMO project, "D4.1 – Initial prototypes of the cyber-threat intelligence gathering,

extraction, sharing components and AI-based solutions. [." 2024. [Online]. Available: https://horizon-dynamo.eu/wp-content/uploads/2025/02/DYNAMO-RPT-D41-V2-0.pdf

[2] ECHO project, "ECHO Network," Project summary. Accessed: Jun. 03, 2022. [Online]. Available: https://echonetwork.eu/

[3] ISO, "ISO 22301 - Business continuity." International Organization for Standardization, 2019.

[4] R. Steen, O. J. Haug, and R. Patriarca, "Business continuity and resilience management: A conceptual framework," *J. Contingencies Crisis Manag.*, vol. 32, no. 4, pp. 1–13, Sep. 2023, doi: 10.1111/1468-5973.12501.

[5] L. S. R. Supriadi and L. Sui Pheng, "Business Continuity Management (BCM)," *Bus. Contin. Manag. Constr.*, pp. 41–73, Aug. 2017, doi: 10.1007/978-981-10-5487-7_3.

[6] D. Rehak, P. Senovsky, and S. Slivkova, "Resilience of Critical Infrastructure Elements and Its Main Factors," *Systems*, vol. 6, no. 2, p. 21, Jun. 2018, doi: 10.3390/systems6020021.

[7] A. Al-Hawamleh, "Cyber Resilience Framework: Strengthening Defenses and Enhancing Continuity in Business Security," *Int. J. Comput. Digit. Syst.*, vol. 15, no. Mar-24, pp. 1315–1331, Mar. 2024, doi: 10.12785/ijcds/150193.

[8] National Academy of Sciences, *Disaster Resilience: A National Imperative*. Washington D.C.: The National Academies Press, 2012. doi: 10.17226/13457.

[9] A. Ishak and E. Williams, "A dynamic model of organizational resilience: Adaptive and anchored approaches," *Corp. Commun. Int. J.*, vol. 23, no. 2, pp. 180–196, Feb. 2018, doi: 10.1108/CCIJ-04-2017-0037.

[10] R. K. Dickson, "Organizational Resilience as the Springboard for Organizational Success in a Turbulent Business Environment," *Eur. J. Manag. Econ. Bus.*, vol. 2, no. 2, pp. 3–24, Mar. 2025, doi: 10.59324/ejmeb.2025.2(2).01.

[11] I. Linkov *et al.*, "Changing the resilience paradigm," *Nat. Clim. Change*, vol. 4, no. 6, pp. 407–409, 2014.

[12] T. Aven and S. Thekdi, "The Importance of Resilience-Based Strategies in Risk Analysis, and Vice Versa," in *IRGC resource guide on resilience (vol. 2): Domains of resilience for complex interconnected systems*, 2 vols., Trump, Benjamin, M.-V. Florin, and I. Linkov, Eds., Lausanne: EPFL International Risk Governance Center (IRGC), 2018, pp. 33–38. doi: 10.5075/epfl-irgc-262527.

[13] M.-V. Florin and B. Trump, "Resilience in the Context of Systemic Risks: Perspectives from IRGC's Guidelines for the Governance of Systemic Risks," in *IRGC resource guide on resilience (vol. 2): Domains of resilience for complex interconnected systems*, 2 vols., Trump, Benjamin, M.-V. Florin, and I. Linkov, Eds., Lausanne: EPFL International Risk Governance Center (IRGC), 2018, pp. 60–68. doi: 10.5075/epfl-irgc-262527.

[14] F. Petit, "Resilience Assessment in Homeland Security," in *IRGC resource guide on resilience (vol. 2): Domains of resilience for complex interconnected systems*, 2 vols., Trump, Benjamin, M.-V. Florin, and I. Linkov, Eds., Lausanne: EPFL International Risk Governance Center (IRGC), 2018, pp. 118–126. doi: 10.5075/epfl-irgc-262527.

[15] I. Nai-Fovino *et al.*, "A proposal for a European cybersecurity taxonomy," Publications Office, Luxembourg, Technical report EUR 29868, 2019. Accessed: Feb. 15, 2022. [Online]. Available: https://data.europa.eu/doi/10.2760/106002

[16] I.-E. Ene and D. Savu, "Cybersecurity - A Permanent Challenge for the Energy Sector," *Romanian Cyber Secur. J.*, vol. 5, no. 1, pp. 107–119, May 2023, doi: 10.54851/v5i1y202310.

[17] S. T. Hossain, T. Yigitcanlar, K. Nguyen, and Y. Xu, "Cybersecurity in local governments: A systematic review and framework of key challenges," *Urban Gov.*, vol. 5, no. 1, pp. 1–19, Mar. 2025, doi: 10.1016/j.ugj.2024.12.010.

[18] K. Aaltola, H. Ruoslahti, and J. Heinonen, "Desired cybersecurity skills and skills acquisition methods in the organizations," in *Proceedings of the European conference on cyber warfare and security*, Academic Conferences International Ltd, 2022, pp. 1–9. doi: https://doi.org/10.34190/eccws.21.1.293.

[19] Health and Safety Executive, "Introduction to human factors - HSE," Introduction to human factors. Accessed: Dec. 14, 2024. [Online]. Available: https://www.hse.gov.uk/humanfactors/introduction.htm

[20] R. J. Glavin and N. J. Maran, "Integrating human factors into the medical curriculum," *Med. Educ.*, vol. 37, no. s1, pp. 59–64, 2003, doi: 10.1046/j.1365-2923.37.s1.5.x.

[21] W. J. Triplett, "Addressing Human Factors in Cybersecurity Leadership," *J. Cybersecurity*

Priv., vol. 2, no. 3, Art. no. 3, Sep. 2022, doi: 10.3390/jcp2030029.

[22] S. Nifakos *et al.*, "Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review," *Sensors*, vol. 21, no. 15, Art. no. 15, Jan. 2021, doi: 10.3390/s21155119.

[23] K. M. Eisenhardt, "Building Theories from Case Study Research," *Acad. Manage. Rev.*, vol. 14, no. 4, pp. 532–550, Oct. 1989, doi: 10.5465/amr.1989.4308385.

[24] J. Gerring, *Case study research: Principles and practices*, 2nd ed. New York, NY, USA: Cambridge University Press, 2017.

[25] R. K. Yin, *Case study research: Design and methods*, 4th ed., vol. 5. Thousand Oaks, California: SAGE Publications Ltd, 2009.

[26] I. Benbasat, D. K. Goldstein, and M. Mead, "The Case Research Strategy in Studies of Information Systems," *MIS Q.*, vol. 11, no. 3, pp. 369–386, 1987, doi: 10.2307/248684.

[27] Z. Zainal, "Case Study As a Research Method," *J. Kemanus.*, vol. 5, no. 1, Art. no. 1, 2007, Accessed: Aug. 01, 2023. [Online]. Available: https://jurnalkemanusiaan.utm.my/index.php/kemanusiaan/article/view/165

[28] E. Hytönen and H. Ruoslahti, "Business Continuity Management– Building Block of Dynamic Resilience," *Crit. Inf. Infrastruct. Secur. Lect. Notes Comput. Sci.*, pp. 120–134, 2024, doi: 10.1007/978-3-031-62139-0_7.

[29] E. Hytönen and H. Ruoslahti, "A Lens to Examine Communication Through Business Continuity Management," in *Public Relations and Sustainability*, D. Verčič, A. T. Verčič, and K. Sriramesh, Eds., Ljubljana: University of Ljubljana: Faculty of Social Sciences, 2023, pp. 205–216. [Online]. Available: https://www.bledcom.com/

[30] H. Ruoslahti and E. Hytönen, "Academic publications create sustainable knowledge in funded projects," in *Public Relations and Sustainability*, Ljubljana, Slovenia: University of Ljubljana, Faculty of Social Sciences, 2024, pp. 223–232. Accessed: Dec. 13, 2024. [Online]. Available: https://gap-project.eu/publications/deliverables/

[31] T. Savolainen, N. McCarthy, H. Ruoslahti, and K. Neville, "Business Continuity Management of Critical Infrastructures from the Cybersecurity Perspective," presented at the EDUCON 2024 in print, Kos, Greece, 2024.

[32] I. Tikanmäki and H. Ruoslahti, "Enhancing Security Education: A Comprehensive Analysis of Virtualized Learning Approaches in the Study of Hybrid Threats," in *2024 IEEE Global Engineering Education Conference (EDUCON)*, Kos Island, Greece: IEEE, May 2024, pp. 1–6. doi: 10.1109/EDUCON60312.2024.10578927.

[33] J. Heinonen and H. Ruoslahti, "Measuring Societal Impacts of Cybersecurity," *Eur. Conf. Cyber Warf. Secur.*, vol. 23, no. 1, Art. no. 1, Jun. 2024, doi: 10.34190/eccws.23.1.2267.

[34] H. Ruoslahti, E. Hytönen, and L. A. G. Sanchez, "Business Model Canvas and Competition to Understand Exploitation of Cybersecurity Project Results," *Eur. Conf. Cyber Warf. Secur.*, vol. 23, no. 1, Art. no. 1, Jun. 2024, doi: 10.34190/eccws.23.1.2519.

[35] H. Ruoslahti and I. Tikanmäki, "The Social Domain: Resilience of Information-Sharing Networks," *Eur. Conf. Cyber Warf. Secur.*, vol. 23, no. 1, Art. no. 1, Jun. 2024, doi: 10.34190/eccws.23.1.2520.

[36] J. Rajamäki and K. Tiitta, "Implementation of OSINT for Improving an International Finance Sector Organization's Cybersecurity," *Int. Conf. Cyber Warf. Secur.*, vol. 19, no. 1, Art. no. 1, Mar. 2024, doi: 10.34190/iccws.19.1.1977.

[37] I. Tikanmäki, J. Savolainen, and H. Ruoslahti, "The Role of Standards in Enhancing Cybersecurity and Business Continuity Management for Organizations," *Inf. Secur. Int. J.*, vol. 55, no. 1, pp. 63–78, 2024, doi: https://doi.org/10.11610/isij.5523.

[38] I. Tikanmäki and H. Ruoslahti, "Human Factors Make or Break Cybersecurity!," *Inf. Secur. Int. J.*, vol. 55, no. 3, pp. 245–259, 2024, doi: 10.11610/isij.5522.

[39] J. Rajamäki, T. Savolainen, and I. Tikanmäki, "The Effect of EU's Artificial Intelligence Act on Cyber Security Training," in *Futureproofing Engineering Education for Global Responsibility*, Switzerland: Cham: Springer Nature, 2025, pp. 229–238. doi: https://doi.org/10.1007/978-3-031-83523-0_21.

[40] I. Tikanmäki and H. Ruoslahti, "Insights on Human Factors Enhancing Cybersecurity," *Inf. Secur. Int. J.*, vol. 55, no. 3, pp. 225–235, 2024, doi: https://doi.org/10.11610/isij.5506.