Business Continuity Against Cyber Interruptions

Harri Ruoslahti and Eveliina Hytönen
Laurea University of Applied Sciences, Espoo, Finland

harri.ruoslahti@laurea.fi
eveliina.hytonen@laurea.fi

Abstract: Resilience and continuity management have wide societal impacts and are particularly important for critical infrastructure organizations. Organizations face constant risk of cyber incidents. Business continuity management strategies rely increasingly on networks of organizations. The research question of this study is: How to ensure business continuity in case of cyber interruptions? Master's students contributed the practical data collection of the sample, which are 25 interviews of Finnish continuity professionals. This data collection was performed as part of their studies in Continuity management. All interviewees have consented to their answers being used as research data. The analysis is based extracting data to the Data Extraction Table (DET) that was specifically designed, based on the research question of this study. The results show that it is important to create a continuity plan grounded on risk assessment and defined actions for possible disruptions. Secure and up-to-date infrastructures with good security measures are recommended. Backup in secure storage locations and backup systems for critical data help restore data. Also, developing methods to continue essential operations even if ICT systems are unavailable, is advisable. Regular staff training on cyber security, response protocols, identifying potential threats, and clear internal and external communication are needed when hit by a cyber incident. Identifying critical operations and recognizing the most important processes will help prioritize during an interruption, and alternative methods can help to continue essential operations when ICT systems are down. BCM processes offer frameworks that help build organizational resilience and can facilitate efficient responses when encountering critical events.

Key words: Resilience, Business continuity, Cyber interruption, Critical infrastructure

1. Introduction

Organizations today face almost constant risks of critical cyber incidents and cyber-attacks. Cyber incidents have been deemed the foremost business interruptions risks according to the Allianz Risk Barometer for two years now (Allianz Risk Barometer, 2023, 2024). This shows that many organizations have to consider how they approach their business continuity management processes and practices to prepare for and combat cyber interruptions. Resilience and continuity management can have very wide societal impacts and they are particularly important for critical infrastructure organizations (Ruoslahti, 2020; Hytönen & Ruoslahti, 2023).

Cybersecurity threats and attacks have grown in number and are becoming increasingly sophisticated which is why individual, organizational, and societal resilience building activities are increasingly dependent on complex and interlinked cyber systems and the interconnections between them (Michel & King, 2019). Developing resilience and continuity in these systems can be enhanced by the study and improvement of interconnectivity and functions between these networks, and their systems of systems (Linkov et al., 2013).

Resilience building processes need communication and collaboration of social networks (Vos, 2017). Communication contributes to resilience by creating organizational mindsets to enhance a culture that emphasizes situational awareness (Weick & Sutcliffe, 2015). Communication can help promote engagement to the Business Continuity Management (BCM) and its functions (Herbane, Elliot & Swartz, 2004). Effective multistakeholder communication and collaboration build continuity and organizational cyber resilience (Hytönen & Ruoslahti, 2023).

BCM frameworks help identify threats and analyse their possible impacts, which can help build organizational resilience and facilitate efficient response to critical events (BSI 2006; ISO 22301:2019; Herbane, 2016). Sharing information across networks operating in physical, information, cognitive, and social domains provide shared situational awareness that facilitates decision-making (Linkov et al., 2013; Linkov et al., 2014). Basic BCM principles can help manage continuity and improve resilience and these include identifying risks, critical activities, and key personnel, while creating guidelines and procedures, and helping promote open communication (Ruoslahti, 2020). The research question of this study is: How to ensure business continuity in case of cyber interruptions?

2. Cyber Interruptions and Resilience

Based on literature in this field, using modern Information and Communications Technology (ICT) solutions present both opportunities and risks, while noting that stability is needed between them (Vučinić & Luburić,

2022). Securing the operations of critical infrastructure operators may be crucial for a functioning society (Ruoslahti, Rajamäki & Koski, 2018). Cyber-attacks and service disruptions against essential critical systems and their networks are increasing (Pahi, Leitner and Skopik, 2017) and severe disruptions in critical infrastructure operations may impact all of society due to critical infrastructures losing essential functionalities when hit by adverse cyber events (Linkov et al., 2014).

ICT can generate knowledge, process information, and promote organizational learning, all these in turn promote productivity (Hortovanyi and Ferincz, 2015) which is important in building organizational competitiveness (Mihalic and Buhalis, 2013). Today's technologies provide flexible ways to integrate, aggregate, and transfer information to enable open innovation processes (Adamides and Karacapilidis, 2020). People are increasingly dependent on ICT and its many applications are very important for their work and everyday lives (Shoemaker and Conklin, 2011), and as organizations increasingly operate in the cyberworld, their people need current knowledge and timely situational awareness (Pöyhönen et al., 2020). Lack of awareness is preyed upon in many ways and e.g. social engineering can lead to very serious consequences that put entire organisational systems at risk (de La Vallée, 2022). Users generate constantly increasing volumes of data, which means that the need for storage will also continue to grow (Taylor, 2023) and organisations should choose carefully how to securely store and back up their data at reasonable costs (Hasan et al., 2023).

Knowledge flows and organizational learning can be enhanced with ICT (Škerlavaj, Dimovski and Desouza, 2010; Zhao and Kemp, 2013). While knowledge transfers can be promoted by enhancing ICT skills throughout the organization (Salleh et al., 2012) adequate ICT knowledge in the organization can help its people capture, store, and share organizational knowledge which increases the availability of their expertise to the organization and its networks (Im, Porumbescu and Lee, 2013), and absorb state-of-the-art knowledge from external sources (Cupiał et al., 2018). ICT skills can be upgraded by proper trainings (Conkova, 2013; Isidro-Filho et al., 2013) and building these skills and competences should recognize the previously adopted competences of learners with the of aim helping them navigate the cyber domain (Aaltola and Taitto, 2019).

Continuity and resilience can be enhanced among various network actors through complex co-creative interactions and even resource integration (Pinho, et al., 2014). Building resilience requires collaboration between social networks; knowledge and meanings become co-constructed through the various interactions between the multiple stakeholders, who participate in it (Vos, 2017). Situational intelligence is also needed to build resilience, which is why the role, engagement, and responsibilities of each network actor, with the mutual interactions and impacts within the network are key factors in network collaboration (Pirinen, 2017). The European Union (EU) Network and Information Security (NIS) Directive calls for strong Public Private Partnership (PPP) collaboration in the critical field of cyber security between authorities and the private sector (European Commission, 2016). There is a recognized need for interoperability with capabilities to supplement for other critical infrastructure providers (Tikanmäki and Ruoslahti, 2017) and deeper collaboration between different actors, such as industry and authorities (Ruoslahti and Hyttinen, 2016).

Today's e-business era emphasizes business continuity (or business continuance) as a structured way for

the organization to have the ability to continue with its operations and services despite some sort of failure or disaster on its computing platform (Bajgoric, 2014). Combining business continuity management (BCM) with systematic Cyber Threat Intelligence (CTI) activities can enhance situational awareness and support decision-making during the stages of the resilience cycle (Hytönen, Rajamäki and Ruoslahti, 2023). Many modern systems include complex interconnections relationships between multiple social and technical subsystems demonstrating seamless integration between computational, human, and physical elements (Broy and Geisberger, 2011). Cyber-Physical Systems (CPS) include inputs and outputs between cyber, physical, and social worlds, when computational elements interact with technical, ecological, organizational, and human elements through cyber networks and the Internet (Amir and Kant, 2018; Murakami, 2012). Server operating platforms could be enhanced with fault and disaster-tolerant technologies so that they can continue to operate even in case of several types of cyber failures or disasters (Bajgoric, 2014). Technological impacts of CPS are very relevant to the resilience of critical infrastructure (Leveson et al., 2017), disaster management (Dahlberg, et al., 2015) and healthcare (Rajamäki and Pirinen, 2017).

CTI activities predict and track cyber domain threats, risks, and opportunities that guide decision making at all levels of the organization, which helps prevent, detect, and respond to cyber-attacks (Shin and Lowry, 2020). Analysis tools may utilize an event management cycle combining elements of business continuity management and of cyber threat intelligence (Hytönen and Ruoslahti, 2023) through the entire event management cycle e.g. prepare, prevent, and protect, absorb, recover, and learn and adapt (Hiermaier et al., 2019; Linkov, 2013).

3. Method

This study uses a case study approach (Yin, 2003) and qualitative research methods for data collection and analysis. The data are collected by conducting interviews and observing interactions (Denzin and Lincoln 1994). This research and its research question (How to ensure business continuity in case of cyber interruptions?) focuses on practitioner interests using an academic approach, as is recommended in the research approach by Baskerville and Myers (2009).

Master's students from Laurea University of Applied Sciences contributed to the practical collection of the sample data, that is, 25 interviews of Finnish continuity professionals. The interviews were conducted during the spring term of 2022, as part of their studies in Continuity management. Each interviewee was asked for informed consent before the start of the interview and only data from interviewees who had consented were included in the final sample.

The cross-case analysis of this data was conducted by the authors in 2024. The analysis is based on narrowing the sample and extracting data to the Data Extraction Table (DET) that was specifically designed, based on the research question of this study. Artificial intelligence, i.e., the ChatGPT4 chatbot, was also used to help identify categories and foci from the respondents' answers.

4. Results

The results indicate that threats are rapidly evolving, and it can be challenging to stay updated on the latest threats and vulnerabilities, and accordingly adapt one's organizational security practices to the changing threat environment. The respondents suggest that organizations firstly take proactive measures, secondly invest in appropriate security infrastructure, and thirdly develop the human element.

4.1 Proactive Measures

The two main proactive measures that were mentioned were completing Risk Assessments (RA) and Business Continuity Plans (BCP). Active RA emphasizes the need to regularly assess the risk profile of the organization by identifying potential cyber threats, their impacts on specific areas of the organization, and the likelihood of their occurrence. Mitigation strategies can be more easily developed against risks that are understood.

A well-defined BCP plan is seen to be a crucial element. A BCP should outline what steps should be taken in case of a cyber incident. According to the respondents, these include identifying critical operations, recovery procedures, communication protocols, and clearly defined roles and responsibilities.

Identifying one's critical operations help determine which services, systems, and data are most essential to the continued functioning of the organization. Recovery procedures should be established for restoring critical systems and data. Communication protocols help outline how to communicate with employees, customers, and other stakeholders during the disruption. Clearly defined roles and responsibilities are needed so that everyone's responsibilities are clear during a cyber incident.

4.2 Security Infrastructure

Security infrastructures that were recommended by the respondents include secure networks, backup systems, and secure storage. Secure networks were deemed extremely important. These may include firewalls, intrusion detection systems, secure network protocols, and robust backup systems.

Firewalls block unauthorized access to the network. Antivirus software detect and remove malware. Intrusion detection and prevention systems monitor for suspicious activity and take action to prevent intrusions. Secure network protocols use strong encryption and authentication protocols to protect data in transit.

Respondents also recommend implementing robust backup systems. These may include regular backups that should be performed frequently enough to minimize data loss and off-site backups to store backup data in a separate location from the primary systems to protect them from an event, which can be a cyberattack or physical, that may affect the primary location. Secure storage ensures that critical data is stored securely, using appropriate encryption and access control measures.

4.3 Human Element

The main human elements that were discussed were staff training and communication. The interviewees emphasized the importance of training one's staff on cyber security. Training can create awareness of cyber security incidents. It is important to educate employees on how to identify and avoid cyber threats, such as the

increasingly common phishing scams and social engineering attempts. Training security policies and incident response help in sharing information about reporting suspicious activities and following established incident response procedures.

Clear and timely communication was deemed to be critical during a cyber incident. The interviews highlight the need for internal communication that keeps employees informed about the situation, response measures, and any necessary changes to work procedures. External communication focuses on communicating with customers, suppliers, and other stakeholders about what are the potential impacts and what steps are and will be taken to address the situation. The interviewees also point out that external expertise can be valuable for building resilience against cyber threats. Organizations should consider collaborating with knowledgeable external partners, such as Network Operations Centres (NOC) and Security Operations Centres (SOC) for added expertise.

4.4 Additional Considerations

Some additional considerations raised by the interviewees are redundancy in key operations and in communication channels. The respondents also mentioned the importance of outsourcing. The results highlight that cyber security is an ongoing process, where organizations need to constantly monitor their security posture and adapt to new and evolving threats.

Redundancy in key operations can include backup systems, such as having multiple backup systems for critical data, and redundant communication channels can be for example phone lines and satellite connections to ensure connectivity. Results show that outsourcing may be important for many organizations that are increasingly reliant on external service providers.

Cost vs. value needs to be actively assessed, as it is essential to invest in adequate security measures that best protect the organization. Cyber security can be expensive, however recognising that the cost of a cyber incident gone bad can be even far greater. It is important to carefully review all contracts with service providers to ensure that they have appropriate security measures and business continuity plans in place, and to verify vendor security by assessing the security practices of each service provider to ensure that they meet the cyber security standards of the organization. Some key takeaways from the interview results on how to ensure business continuity in case of cyber interruptions are presented below (Table 1):

Table 1: Results on business continuity measures in case of cyber interruptions.

Category	Measures to ensure business continuity
Preparedness	Create and update a continuity plan that is based on risk assessments and defines actions for disruptions
Secure infrastructure	Use reliable and up-to-date ICT systems and software and good security measures (antivirus, firewalls)
Backup	Invest in secure storage locations and backup systems for critical data
Staff training	Regularly train staff on cyber security, response protocols, and to identify potential threats
Communication	Ensure clear communication channels for internal and external communication during a cyber incident
Critical operations	Recognize which processes are most important and need to be prioritized during an interruption
Alternative methods	Develop methods to continue essential operations, even if ICT systems are unavailable
Risk assessment	Regularly review organizational risk profile, assess potential threats and implement mitigation measures

As seen above (Table 1) preparedness is key. Preparedness is based on creating a solid BCP. That should be grounded on risk assessments to define actions for possible disruptions. Respondents deemed it important to identify critical operations recognizing which processes are most important and will need to be prioritized during an interruption. Risk assessments are recommended to be carried out regularly to review the risk profile of the organization, and to assess potential threats and implement mitigation measures. Secure ICT infrastructures, such as reliable and up-to-date ICT systems and software, with good security measures (e.g. antivirus, firewalls) are needed, and investing in backup helps having needed secure storage locations and backup systems for critical data.

Alternative methods (e.g. paper-based systems) can and should be developed to enable continuing essential operations, even if ICT systems should become unavailable. Recognizing the human element and conduct staff

training regularly on cyber security, response protocols, and how to identify potential threats was indicated in the results. Clear communication channels are needed for internal and external communication when hit by a cyber incident.

5. Conclusions

Based on the results, it is important to note that cyber security is deemed a complex and ever-evolving field. Recommendations for cyber incident awareness and management can be derived by comparing the responses of the interviews with literature (Table 2).

Table 2: Literature vs. results: how to ensure business continuity in case of cyber interruptions.

Category	Measures to ensure business continuity	Literature
Preparedness	Create and update a continuity plan that is based on risk assessments and defines actions for disruptions	BCM processes identify threats and analyse their possible impacts on an organization (Herbane, 2016)
Secure infrastructure	Use reliable and up-to-date ICT systems and software and good security measures (antivirus, firewalls)	Technological impacts of CPS are very relevant to the resilience of critical infrastructure (Leveson et al., 2017)
Risk assessment	Regularly review organizational risk profile, assess potential threats, and implement mitigation measures	Identifying risks, critical activities, and key personnel (Ruoslahti, 2020)
Staff training	Regularly train staff on cyber security, response protocols, and to identify potential threats	People need current knowledge and timely situational awareness (Pöyhönen et al., 2020); ICT skills can be upgraded by proper trainings (Conkova, 2013)
Communication	Ensure clear communication channels for internal and external communication during a cyber incident	Communication supports BCM functions when responding to a critical incident (Vos, 2017)
Critical operations	Recognize which processes are most important and need to be prioritized during an interruption	Identifying critical activities, and key personnel (Ruoslahti, 2020)
Alternative methods	Develop methods to continue essential operations, even if ICT systems are unavailable	Business continuity is the ability to continue with operations despite failure in computing (Bajgoric, 2014)
Backup	Invest in secure storage locations and backup systems for critical data	The need for storage will continue to grow (Taylor, 2023)

As seen above (Table 2), preparedness includes a continuity plan that is based on risk assessments and is updated regularly to define what actions should be taken in case of disruptions. Implementing BCM processes provides a structured framework to identify threats and analyse their possible impacts on an organization (e.g. Herbane, 2016; Ruoslahti, 2020), through the entire event management cycle (e.g. Hiermaier et al., 2019; Linkov et al., 2013). The results of this study imply, that risk assessment should include a regular review of the organizational risk profile and assess the impacts of potential threats so that appropriate mitigation measures can be selected and implemented. An important part of BCM is identifying one's critical operations. This means recognizing which processes are most important and need to be prioritized during an interruption (e.g. Linkov et al., 2013; Ruoslahti, 2020). Based on the results, alternative methods that can help continue essential operations, even when ICT systems become unavailable, are needed. For example, the Resilience Matrix can serve as a tool that helps focus on shared situational awareness to facilitate decision-making and sharing of information across networks (Linkov et al., 2013).

Managing business continuity and building resilience is a process that needs communication and collaboration between social networks (e.g. Vos, 2017; Ruoslahti, 2020; Linkov et al., 2013). People need current knowledge and timely situational awareness (e.g. Pöyhönen et al., 2020); ICT skills can be upgraded by proper trainings (e.g. Conkova, 2013). The results show, that to support business continuity management in the face of cyber interruptions, regularly training staff on cyber security, response protocols, and on identifying and reporting potential threats is an important way of enhancing situational awareness and communicating about continuity activities in an organisation (e.g. Weick & Sutcliffe, 2015; Herbane, Elliot & Swartz, 2004). Based on the results, clear and functioning communication channels for internal and external communication during cyber incidents are needed. Ensuring clear communication channels for internal and external communication help keep staff

and stakeholders informed of the situation and of needed response measures. Collaboration and communication enable monitoring the context and developing collective responses (e.g., Vos, 2017; Sánchez & De Batista, 2023).

Future research is recommended to address gaps in understanding collaboration between human factors and technological solutions to ensure business continuity in the context of growing cyber threats. Research on integrating and aligning cyber security and BCM principles could provide organisations with integrated frameworks and guidelines on how to build cyber resilience. Knowledge is needed on best practices in responding to different cyber incidents. This research should also address the human element in cyber resilience and business continuity management. Topics for the research could be for example, cyber risk communication, and training practices and their effects in an organisation, and internal and external communication in managing a cyber incident.

Acknowledgement

This study has received funding by the European Union projects ECHO, which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no. 830943, and DYNAMO, under grant agreement no. 101069601. The views expressed are those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

References

Aaltola, K. and Taitto, P. (2019) *Utilising Experiential and Organizational Learning Theories to Improve Human Performance in Cyber Training*, Information & Security: An International Journal, 43(2), pp. 123–133. doi: 10.11610/isij.4311.

Adamides, E. and Karacapilidis, N. (2020). *Information technology for supporting the development and maintenance of open innovation capabilities*, Journal of Innovation & Knowledge, 5(1), pp. 29-38.

Allianz Risk Barometer (2024) Allianz Global Corporate & Specialty (AGCS), https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2024.pdf.

Allianz Risk Barometer (2023) Allianz Global Corporate & Specialty (AGCS), https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2023-press.html, last accessed 2023/11/28.

Amir, S., and Kant, V. (2018) *Sociotechnical resilience: A preliminary concept*, Risk Analysis, 38(1), pp. 8-16.

Baskerville, R. L. and Myers, M. D. (2009) *Fashion waves in information systems research and practice*, Mis Quarterly, pp. 647-662.

Bajgoric, N. (2014). *Business continuity management: a systemic framework for implementation*, Kybernetes, 43(2), pp. 156-177.

British Standards Institution. (2006) *BS 25999-1 Code of practice for business continuity management,* London: British Standards Institution.

Broy, M. and Geisberger, E. (2011) *Cyber-physical systems, driving force for innovation in mobility, health, energy and production*, Acatech: The National Academy of Science and Engineering, Munich.

Cupiał, M., Szeląg-Sikora, A., Sikora, J., Rorat, J. and Niemiec, M. (2018). *Information technology tools in corporate knowledge management,* Ekonomia i prawo. Economics and law, *17*(1), pp. 5-15.

Conkova, M. (2013) *Analysis of Perceptions of Conventional and E-Learning Education in Corporate Training*, Journal of Competitiveness, 5(4), pp. 73–97, doi: 10.7441/joc.2013.04.05.

Dahlberg, R., Johannessen-Henry, C., Raju, E. and Tulsiani, S. (2015) *Resilience in disaster research: Three versions*, Civil Engineering and Environmental Systems, *32*(1-2), pp. 44–54.

Denzin, N. K. & Lincoln, Y. S. (1994) *Handbook of Qualitative Research*, Sage Publications, Thousand Oaks, USA.

de La Vallée, P., Iosifidis, G., Rossi, A., Dri, M., & Mees, W. (2022, October). Sector-Specific Training-A Federated Maritime Scenario. In International Conference on Multimedia Communications, Services and Security (pp. 21-35). Cham: Springer International Publishing.

European Commission (2016) *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union*, [Online] Available at: https://eurlex.europa.eu/eli/dir/2016/1148/oj.

Hasan, M. Z., Sarwar, N., Alam, I., Hussain, M. Z., Siddiqui, A. A. and Irshad, A. (2023). Data recovery and backup management: A cloud computing impact. In 2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T) (pp. 1-6). IEEE.

Herbane, B. (2016). A Business Continuity Perspective on Organisational Resilience, in Resource Guide on Resilience, EPFL International Risk Governance Center, Lausanne, available at https://www.irgc.org/irgc-resourceguide-on-resilience/

Herbane, B., Elliot, D. and Swartz, E.M. (2004) *Business Continuity Management: Time for a Strategic Role?* Long Range Planning 37(5), pp. 435-457.

Hortovanyi, L. and Ferincz, A. (2015) *The impact of ICT on learning on-the-job*, The Learning Organization, 22(1), pp. 2–13. doi: 10.1108/TLO-06-2014-0032.

Hytönen, E., Rajamäki, J., and Ruoslahti, H. (2023) *Managing Variable Cyber Environments with Organizational Foresight and Resilience Thinking*, in International Conference on Cyber Warfare and Security, 18(1), pp. 162-170).

Hytönen, E. and Ruoslahti, H. (2023) A Lens to Examine Communication Through Business Continuity Management. In Proceedings of the 30th International Public Relations Research Symposium BledCom, EDS: Dejan Verčič, Ana Tkalac Verčič and Krishnamurthy Sriramesh, University of Ljubljana, pp. 205 - 216. AVAILABLE: https://www.bledcom.com/

Im, T., Porumbescu, G. and Lee, H. (2013) *ICT as a Buffer to Change*, Public Performance & Management Review, 36(3), pp. 436–455. doi: 10.2753/PMR1530-9576360303.

Isidro-Filho, A., Guimarães, T. D. A., Perin, M. G., and Leung, R. C. (2013). *Workplace learning strategies and professional competencies in innovation contexts in Brazilian hospitals,* BAR-Brazilian Administration Review, *10*, 121-134.

ISO 22301:2019. Societal security - Business continuity management systems - Requirements. Helsinki: Finnish Standards Association SFS.

Leveson, N., Dulac, N., Zipkin, D., Cutcher-Gershenfeld, J., Carroll, J., & Barrett, B. (2017). *Engineering resilience into safety-critical systems*, In Resilience engineering (pp. 95-123). CRC Press.

Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., ... and Thiel-Clemen, T. (2014). *Changing the resilience paradigm,* Nature climate change, *4*(6), pp. 407-409.

Linkov, I., Eisenberg, D.A., Bates, M.E., Chang, D., Convertino, M., Allen, J.H., Flynn, S.E. and Seager, T.P. (2013) *Measurable resilience for actionable policy*, Environmental Science and Technology, 47(18), pp. 10108-10110.

Michel, M. C. K. and King, M. C. (2019) *Cyber Influence of Human Behavior: Personal and National Security,Privacy, and Fraud Awareness to Prevent Harm*, In 2019 IEEE International Symposium on Technology and Society (ISTAS), pp. 1-7.

Mihalic, T. and Buhalis, D. (2013) *ICT as a new competitive advantage factor – case of small transitional hotel sector*, Economic and Business Review, 15(1), pp. 33–56.

Murakami, K.J. (2012) *CPSS (Cyber-physical-social systems) initiative - Beyond CPS (Cyber-physical systems) for a better future*, [online], Grid Consortium Japan, http://www.jpgrid.org/event/2011/ws34_murakami.pdf.

Pahi, T., Leitner, M. & Skopik, F. (2017) *Analysis and Assessment of Situational Awareness Models for National Cyber Security Centers*, ICISSP, pp. 334-345.

Pinho, N., Beirão, G., Patrício, L. and Fisk, R. (2014) *Understanding value co-creation in complex services with many actors*, Journal of Service Management, 25(4), pp. 470-493.

Pirinen, R. (2017) *Towards Common Information Systems Maturity Validation - Resilience Readiness Levels (ResRL)*, Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management - Volume 3: ISE, pp. 259 -266.

Pöyhönen, J., Rajamäki, J., Ruoslahti, H. and Lehto, M. (2020). *Cyber situational awareness in critical infrastructure protection,* Annals of Disaster Risk Sciences*: ADRS*, *3*(1), 0-0.

Rajamäki, J. and Pirinen, R. (2017) *Design science research towards resilient cyber-physical eHealth systems*, Finnish Journal of eHealth and eWelfare, 9(2–3), pp. 203–216.

Ruoslahti, H. (2020). *Business Continuity for Critical Infrastructure Operators*, Annals of Disaster Risk Sciences, Special issue on cyber-security of critical infrastructure, 3(1). Available: https://ojs.vvg.hr/index.php/adrs.

Ruoslahti, H. and Hyttinen, K. (2016) *A Co-created Network Community for Knowledge and Innovations – Promoting Safety and Security in the Arctic*, Proceedings of the 23rd International Public Relations Research Symposium BledCom, Faculty of Social Sciences, Ljubljana, pp. 100–106.

Ruoslahti, H., Rajamäki, J. and Koski, E. (2018) *Educational competences with regard to resilience of critical infrastructure*, Journal of Information Warfare. Journal of Information Warfare, 17(3), pp. 1-16.

Salleh, K., Chong, S. C., Syed Ahmad, S. N. and Syed Ikhsan, S. O. S. (2012). *Learning and knowledge transfer performance among public sector accountants: an empirical survey,* Knowledge Management Research & Practice, *10*(2), pp. 164-174.

Sánchez, M. A. and De Batista, M. (2023). *Business continuity for times of vulnerability: Empirical evidence,* Journal of contingencies and crisis management, 31(3), pp. 431-440.

Shin, B., and Lowry, P. B. (2020) *A review and theoretical explanation of the 'cyberthreat-intelligence (cti) capability that needs to be fostered in information security practitioners and how this can be accomplished*, Computers & Security, 92, 101761. https://doi.org/10. 1016/j.cose.2020.101761

Shoemaker, D. and Conklin, W. A. (2011) *Cybersecurity: The Essential Body of Knowledge*, Boston, MA: Cengage Learning.

Škerlavaj, M., Dimovski, V. and Desouza, K. C. (2010) *Patterns and structures of intra-organizational learning networks within a knowledge-intensive organization*, Journal of Information Technology, 25(2), pp. 189–204. doi: 10.1057/jit.2010.3.

Taylor, A. R. E. (2023). *Cloud Backup and Restore: The Infrastructure of Digital Failure, in Routledge International Handbook of Failure*. Taylor & Francis.

Tikanmäki, I. and Ruoslahti, H. (2017) *Increasing Cooperation between the European Maritime Domain Authorities*, *International Journal of Environmental Science*, 2, pp. 392–399.

Vos, M. (2017) *Communication in Turbulent Times: Exploring Issue Arenas and Crisis Communication to Enhance Organisational Resilience*, Jyväskylä University School of Business and Economics, N:o 40 / 2017.

Vučinić, M., and Luburić, R. (2022) "*Fintech, risk-based thinking and cyber risk*", *Journal of Central Banking Theory and Practice*, 11(2), pp. 27-53.

Weick, K. and Sutcliffe K. (2015). *Managing the Unexpected: Sustained Performance in a Complex World.* Hoboken: John Wiley & Sons.

Yin, R. K. (2003) *Case Study Research, Design and Methods,* 3rd. Ed. Sage, Thousand Oaks, USA.
Zhao, F. and Kemp, L. (2013) *Exploring individual, social and organisational effects on Web 2.0-based workplace learning: a research agenda for a systematic approach*, *Research in Learning Technology*, 21. doi: 10.3402/rlt.v21i0.19089.