# Managing Variable Cyber Environments with Organizational Foresight and Resilience Thinking

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

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

**Abstract:** Combining business continuity management (BCM) and systematic cyber threat intelligence (CTI) can improve cyber situational awareness to support decision-making through the phases of the resilience cycle (plan, absorb, recover, adapt) to ensure the continuity of organizational operations when encountered by cyber disruptions. End-user needs, human factors, high ethical standards, and social impacts can best be adapted when professionals from different fields work together with end-users to refine and co-develop selected tools into a platform. A resilience assessment that combines BCM and CTI enables 1) quick or detailed assessment of the investigated industry and its critical processes, 2) measurement of performance goals based on information received from end users, where artificial intelligence-based self-learning approaches can be used for functional descriptions, 3) information on the sensitivity of the investigated industry and vulnerability and 4) resilience and BCM throughout the entire resilience cycle. A new Horizon Europe project DYNAMO (Dynamic Resilience Assessment Method including a combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors) works towards combining BCM and CTI to generate a situational picture for decision support. Having this in mind, certain cybersecurity and BCM tools will be developed, refined, and integrated into the DYNAMO platform to provide decision support and awareness to chief information security officers, cybersecurity practitioners, and other stakeholders. This paper reports a case study that explores how combining CTI and BCM can help in the case of a cyber-attack. The research material consists of the news articles by the largest newspaper in Finland, Helsingin Sanomat (HS) of how the cyber attack against the therapy center Vastaamo progressed during the first week after the attack. The results show that cyber threat intelligence when flexibly integrated into the BCM approach could create better conditions for improved organizational foresight to react to unpredictable cyber threats to ensure business continuity.

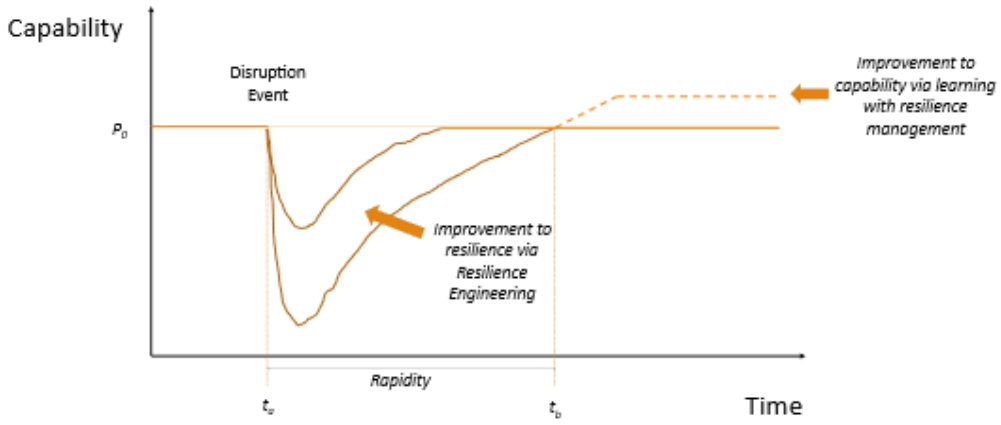
**Keywords**: Cyber Threat Intelligence, Business Continuity Management, Resilience, Situational Awareness

## 1. Introduction

Business continuity management (BCM), crisis management (CM), disaster recovery (DR), and resilience are related concepts, the purpose of which is to secure the critical functionality of the system in all situations. Risks and crises are often a derivative of external stressors, while the organization's resilience is more intrinsic, and in this sense, the priority of preventive behaviour at the organizational level is the preparation of various procedures to respond to crises or critical events (Linkov et al., 2014). Traditionally, BCM combines risk management and quality management. DR involves the re-establishment of systems and functions to recover from a disaster. The BC Plan lists the steps to be taken to ensure the continuity of critical business operations. (Sawalha, 2021.)

Figure 1 presents the management cycles of BCM and resilience management. The holistic BCM process identifies potential threatening impacts on the organization and provides a framework for developing resilience and the ability to respond effectively to protect the system and the interests of the key actors. The goal of resilience engineering is to improve resilience by reducing the drop in capability and speeding up recovery. The goal of resilience management is to learn from unwanted events and thus improve the system's capability.

*a) Business continuity cycle*




*b) Resilience cycle and aspects of resilience engineering*

**Figure 1: Business continuity and resilience cycles**

Resilience can be understood as business flexibility, endurance, or ability to recover from adverse events; an ability to recover or adapt to a new normal after a crisis or a critical event. The measure of resilience is the ability of an organization to minimize any negative impacts. Thus, resilient organizations can quickly adapt to wide systemic changes occurring in the organization, its value network, or impacting the entire society. Resilient organizations or networks have organizational stability, agility, and a culture that promotes situational awareness to detect and identify clues that may indicate the realization of risks for appropriate mitigation and reaction. (Palomäki, Roschier, Gilbert and Pokela, 2020.)

Examples of threats against critical infrastructures and vital societal services are numerous. The WannaCry attack in 2017 encrypted data and files on 230 000 computers in 150 countries and impaired the functionality of the National Health Service (NHS) in England (Ghafur et al., 2019), a cyber-attack halted the network of a Czech hospital in 2021 (Muthuppalaniappan and Stevenson, 2021), and in 2021 South Africa's port and rail operator, Transnet, experienced a cyberattack that caused a standstill in the movement of goods in some of its ports (South Africa Autos Report, 2021). A Finnish private psychotherapy service provider, Vastaamo, experienced cyber-attacks in 2018, 2019 and 2020, as the attacker stole thousands of records and then tried to blackmail individual patients directly threatening to expose documents containing everything from personal identity codes to therapy session transcripts (Tuttle, 2021). The financial losses forced Vastaamo to declare bankruptcy and close (Whitney, 2021).

The examples demonstrate vulnerabilities of critical services and how cyber threats may impact their business continuity. Systems that combine principles of business continuity with cyber threat warning systems can promote better preparedness and cyber resilience against cyber incidents. The goal of project DYNAMO is to combine cyber threat intelligence (CTI) and business continuity management (BCM) to generate a situational picture for decision support of critical sectors (DYNAMO, 2022). This study looks at the cyber-attack against the therapy center Vastaamo. The study adds in part to the practical body of knowledge that the DYNAMO project cumulates. The research question is: "*How to promote business continuity during cyber incidents*?".

## 2. Literature

Cyber security is still a young field of study, a consensus on the scientific definition of the term is lacking, but there is a common understanding that cyber security investigates how to secure cyberspace from threats and damage (Edgar and Manz, 2017). The Finnish security commission (Turvallisuuskomitea) defines cyber security as a state where cyberspace can be trusted, and its functions become secured (Turvallisuuskomitea, 2018).

The National Initiative for Cybersecurity Careers and Studies (NICCS) defines cybersecurity as "[t]he activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation" (NICCS, 2017). Dalal et al. (2021, p. 4) include the human-factor in the definition of cyber security, more specifically the definition of organizational cyber security as "the efforts organizations take to protect and

defend their information assets, regardless of the form in which those assets exist, from threats internal and external to the organization".

Cyberspace can be defined in many ways. This study understands it as an entity that combines three viewpoints in the field of research: information, technology, and social viewpoint as presented in the Figure 2. The healthcare system with its various information systems is an example of cyberspace (Lehto, Pöyhönen and Lehto, 2019).

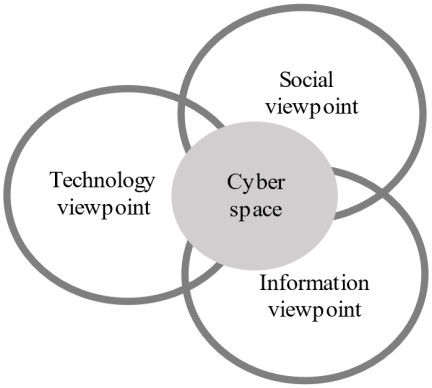



**Figure 2: The dimensions of cyberspace (modified Edgar and Manz, 2017)**

The basis of business continuity management is to combine risk and quality management principles based on probability-based quantitative methodology, which is useful in calculating predictable or calculable stress situations. However, securing systems with risk and business management-based solutions may be unrealistic for many systems for two reasons: (1) current interconnected social, technical, and economical networks form such complex systems that considering all possible risks may be very time-consuming and costly; (2) they may consider only events that are known or have happened before. (Linkov et al., 2014.)

The concept of resilience is based on two very different scientific traditions: (1) psychology, where resilience is referred to as affecting how an individual recovers from personal trauma or crisis; (2) Ecological systems thinking that looks at resilience as a nonlinear dynamics of recovery or adaption. Later resilience has been used in studies looking at ecosystems management, sustainable development, climate change, and politics. (Linkov and Kott, 2018.)

National Academy of Sciences (2012) define resilience as "the ability to prepare and plan for, absorb, recover from, or more successfully adapt to actual or potential adverse events". On the organizational level, the term 'resilience' can describe the inherent characteristics of the organizations that can respond more quickly, recover faster, or develop more unusual ways of doing business under pressure than others (Vogus and Sutcliffe, 2007). Resilience can also be seen as the capability of a system to recover in the middle of shocks or stressful events over time (Palma-Oliveira and Trump, 2016). In a system (e.g., an organization) there are multiple different levels that are interrelated. This implies interaction between those levels that can be called factors and sub-systems (Palma-Oliveira and Trump, 2016) or domains (Linkov et al., 2013). Herbane (2016) states that in the field of economics, resilience is often characterized as the aspiration or aim of business continuity management systems, or as the articulation of the future state of organization following achievement of its strategy. Business Continuity Management is one of several activities to support resilience.

A systems approach to resilience can be described and analysed using the Resilience Matrix, that maps system domains across an event management cycle of resilience functions (Linkov, 2013). The event management cycle or the resilience cycle can be simplified into four functions: plan, absorb, recover, and adapt. Decision-making can benefit from using the phases of resilience by developing e.g., measurement methods and practices, which can be used to assess the threats, probabilities, and impacts on the critical functions of the organizations (Juntunen, 2014).

Cyber threat intelligence (CTI) is actionable threat information that is relevant to a certain organization and that requires careful attention. CTI consists of activities such as acquiring, processing, and analyzing threat information to identify, track, and predict threats, risks, and opportunities inside the cyber domain, and thus to engineer more precise defense strategies. CTI can have a crucial role in directing organisational behaviour in

prevention, detection, and response to cyber-attacks. It can enable better decision making at different levels in the organization, including the strategic, tactical, and operational levels. (Shin and Lowry, 2020.)

Kotsias et al. (2022) state that even though firms are fully compliant with industry "best practice" cyber security standards, they may not be able to cope with well organised, sophisticated cyber-attacks. Leveraging cyber-threat intelligence (CTI) to direct cyber-defence is key in resolving the asymmetry. The adoption of CTI can pose many challenges to companies. There might be limited knowhow about the deployment and use of CTI. Moreover, many organizations would need to transform their cybersecurity practice from a reactive logic towards a proactive logic driven by CTI.

## 3. Methodology

Case study research aims at providing deep and detailed information on the subject of the case study to support development activities. Development work is based on prior theories, knowledge, and study that deal with similar problems as the study at hand. Case study often aims at answering the questions 'how?' and 'why?'. The case study takes into account the connections and social situations in time and space. A case study is a well-suited approach when trying to deeply understand the situation of the case organization by studying it in its own environment to produce a solution to a given problem or provide researched development suggestions (Yin, 2009).

This case study builds on the news articles by the largest newspaper in Finland, Helsingin Sanomat (HS) of how the cyber attack against the therapy center Vastaamo progressed during the first week. The material is a sample of 16 HS articles between 24.10. – 29.10.2020. To answer the research question, relevant data were extracted into a table that was specifically developed for this study.

## 4. Case cyber-attack against Vastaamo

The results of this case study are based on 16 publicized newspaper articles on how the attack progressed during the first news week (see Figure 3). These articles deal with how the cyber-attack and ransom case, the ensuing police investigation, and the reactions and situation of the victims evolved. This part briefly presents the sample articles.

**Table 1: Articles published in Helsingin Sanomat between 24 October and 29 October in 2020**

| Articles published in Helsingin Sanomat between 24 October and 29 October in 2020 | | | |
|---|---|---|---|
| **Article** | **Date** | **Title (translations by the authors)** | **Title in Finnish** |
| 1 | 24.10. | Cyber-attack against Vastaamo got hackers chasing the thief | Vastaamon tietomurto sai hakkerit jahtaamaan varasta |
| 2 | 24.10. | This feels extremely hurtful | Tuntuu äärimmäisen loukkaavalta |
| 3 | 25.10. | Cowardly to blackmail with hacked patient information | Hakkeroiduilla potilastiedoilla kiristäminen on raukkamaista |
| 4 | 25.10. | Customers blackmailed directly | Asiakkaita kiristetty suoraan |
| 5 | 26.10. | Data breach reported weeks after notifying police | Murrosta tiedotettiin viikkoja rikosilmoituksen jälkeen |
| 6 | 26.10. | Experts: data breach victims in the thousands | Asiantuntijat: Tietomurron uhreja on jopa tuhansia |
| 7 | 26.10. | Strong feelings at this moment are insecurity and disbelief | Vahvoja tunteita tällä hetkellä ovat turvattomuus ja epäusko |
| 8 | 27.10. | Psychotherapy centre Vastaamo has a bad reputation in its field | Psykoterapiakeskus Vastaamolla on alalla jopa surkea maine |
| 9 | 27.10. | Data breach did not surprise healthcare actors | Tietomurto ei yllättänyt sote-alan toimijoita |
| 10 | 27.10. | Forensic psychologist: exceptionally shrewd case | Oikeuspsykiatri: Tapaus on poikkeuksellisen häikäilemätön |
| 11 | 28.10. | Damages may take years | Vahingonkorvauksia voi joutua odottamaan vuosia |

| Articles published in Helsingin Sanomat between 24 October and 29 October in 2020 | | | |
|---|---|---|---|
| **Article** | **Date** | **Title (translations by the authors)** | **Title in Finnish** |
| 12 | 28.10. | Psychotherapist: important now to support victims | Psykoterapeutti: Uhrien tukeminen on nyt tärkeää |
| 13 | 28.10. | Ideas on how to help the victims | Keinoja tietomurron uhrien avuksi ideoidaan |
| 14 | 29.10. | Vastaamo may be the largest crime skein in Finland | Vastaamo voi olla isoin rikosvyyhti Suomessa |
| 15 | 29.10. | F-Secure trying to track Vastaamo blackmailer | F-Secure yrittää jäljittää Vastaamo-kiristäjää |
| 16 | 29.10. | Experts: data breach easy | Asiantuntijat: Tietomurto oli helppo |

**Article 1** HS 24.10.2020 C*yber-attack against Vastaamo got hackers chasing the thief*. Due to the cyber-attack against the psychotherapy center Vastaamo, up to tens of thousands of patients' information is suspected to have ended in the hands of a hostile cyber attacker. Vastaamo confirms the cyber-attack, and that the attacker is demanding 450.000 Euro as bitcoins, or the information of 100 people will be made public on the Internet every day. The police are investigating this as a cyber-attack and a felony of distributing private information. The cyber experts interviewed suspected that the information had perhaps been only secured by a default password and thus, had been quite easily accessible. In their view the Vastaamo network had been neglected (e.g., many network servers had not been updated in years) and network addresses pointing to the patient records or Vastaamo Intranet had been publicly visible. The attacker has notified the attack in a discussion.

**Article 2** HS 24.10.2020 *This feels extremely hurtful.* The psychotherapy center Vastaamo informed its customers about the cyber-attack and ransom request first only on its website. According to the deputy data protection ombudsman this was not effective enough, and that Vastaamo had been ordered to personally inform everyone in their registers. The information of 300 people has been made public in the Tor network. A victim of the cyber-attack, who was interviewed by HS says that he is worried about patient safety and that he is hesitant to see a therapist in the future.

**Article 3** 25.10. *Cowardly to blackmail with hacked patient information*. The hacker removed on Friday (23.10.) the sensitive patient information from the Tor network, and them reloaded them. Apparently, the patient data was insufficiently encrypted, as they could be hacked so easily. This makes it difficult for patients to believe in the privacy of treatment. There is only a minor probability that the attackers are caught. They would have to make a mistake to be caught, says an expert from F-Secure.

**Article 4** 25.10. *Customers blackmailed directly*. Several victims of the data breach have reported that on Saturday (24.10.) at around 19:30 they have received a direct ransom message demanding them to pay Bitcoins in the sum of 200 Euro (if paid within 24 hours) or 500 Euro (if paid within 48 hours). The ransom message states that the victims must pay, because Vastaamo refuses to take responsibility and pay.

**Article 5** HS 26.10. Data breach reported weeks after notifying police. The police notes on Sunday (25.10.) that they have so far received thousands of reports of the data breach crime. The police says that they do not know the nationality or the location of the attacker, and if the ransom messages are sent by the attacker. Vastaamo says, they had reported the crime and notified the Cyber security center, The National Supervisory Authority for Welfare and Health, and the data protection ombudsman as soon as they gained information of what had happened. Vastaamo reveals that customer information may have disappeared already in data breaches in 2018 and 2019. The Ministry of the interior took stand, by informing on Saturday (24.10) that the victims of the data breach need urgent help.

**Article 6** 26.10. *Experts: data breach victims in the thousands*. The blackmailer shared for a while a folder with personal information from up to 2.000 patients in the dark web. The leaked information contains patient names, personal identity numbers, contact information, notes from therapy sessions and medical reports.

**Article 7** 26.10. *Strong feelings at this moment are insecurity and disbelief*. One victim says that it was difficult to find information about what to do. There were no clear instructions before this day. The first days were filled with uncertainty and silence. He has suffered from insomnia and reports seeing a great worry of those who don't have the resources to do anything about this. People are totally devastated; small regrets will not be enough, something bigger must be done.

**Article 8** 27.10. *Psychotherapy center Vastaamo has a bad reputation in its field*. The CEO of Vastaamo was let go because of being suspected of keeping the data breach of the company server a secret for over a year. The ex-CEO claims that the November 2018 breach only became evident when there was an investigation in October

2020. The National Supervisory Authority for Welfare and Health notes that the Vastaamo case has raised the question of a need to strengthen cyber security and the level of its control.

**Article 9** 27.10. *Data breach did not surprise healthcare actors*. An expert from the Association of Finnish Local and Regional Authorities notes that the private operators of the healthcare sector have a lot to develop as cyber security is concerned. The approximately 18.000 companies are of different sizes and may have very different levels of investments in cyber security.

**Article 10** 27.10. *Forensic psychologist: exceptionally shrewd case*. The Head forensic psychologist estimates that the Vastaamo data breach and the ensuing ransom demands are exceptionally shrewd and show an exceptionally far-taken indifference toward weaker people.

**Article 11** 28.10. *Damages may take years*. Responsibility to pay the damages is with people responsible for the data breach, with the attacker (if they are ever caught), with Vastaamo (if it has not complied with data protection regulations), and with those healthcare districts that have bought Vastaamo services. This is a case of distributing information that violates private life, notes a professor of public law. The first step is to determine if the register-holder has acted according to data protection regulations.

**Article 12** HS 28.10. *Psychoterapist: important now to support victims*. The feeling of safety may be become severely disturbed, and it is unrealistic to expect that they all can report the crime, comments a Head of a psychotherapy center. Data breach experts have told that they have seen the information from as many as 2.000 patients.

**Article 13** 28.10. *Ideas on how to help the victims*. The Minister of Justice notes that one way to help the Vastaamo victims could be to provide a rapid change of personal identification numbers. The Ministry of Finance is preparing legislation for expediated change of personal identification numbers.

**Article 14** 29.10. *Vastaamo may be the largest crime skein in Finland*. The National Bureau of Investigation has received over 15.000 reports of crime regarding the Vastaamo data breach and ransom case. The deadlines given by the blackmailer have passed, but the police have no information of the blackmailer taking any new action. The Minister of science and culture has commented that similar data breaches to Vastaamo should never happen again. This data breach has been compared to a major disaster. Customer information regulations have to be changed so that similar companies will have tighter cyber security requirements.

**Article 15** 29.10. *F-Secure trying to track Vastaamo blackmailer*. The cybersecurity company F-Secure is asking Vastaamo victims to contact their research director to collect information on the Bitcoin wallets to try to track where the ransom money has gone. Bitcoin is based on blockchains with unchanged public records of transactions that F-Secure will try to follow.

**Article 16** 29.10. *Experts: data breach easy*. Cybersecurity experts interviewed note that the Vastaamo network had been configured in a way that the data breach could be easily done. When googling for information on Vastaamo, a link to Vastaamo's public materials and references to Vastaamo's own instructions under the name 'Patient register' were easily available. Someone claiming to be the attacker revealed in the dark web that the patient register was obtained by using a default user and passwords. An expert interviewed by the HS found some twenty vulnerabilities in the Vastaamo server programs that pertained to the web address of the patient register.

## 5. Results

Results and conclusions are based on the data collected from the 16 sample articles. The results are discussed in the framework of a resilience cycle with six phases: Prepare, Prevent, Protect, Response, Recover, and Learn/adapt (Figure 4).

**Table 2: Results of the study in the framework of resilience cycle**

| | Prepare | Prevent | Protect | Response | Recover | Learn/adapt |
|---|---|---|---|---|---|---|
| **Cyber Threat Intelligence** | Customer information disappeared already 2018 and 2019 | Vulnerability of today's information society | | Nationality of attacker nnot know<br><br>Notify ransom demand to police | Vastaamo ex-CEO claims 2018 breach became first evident when in October 2020 | Private healthcare operators have a lot to develop as cyber security is concerned |

| | Prepare | Prevent | Protect | Response | Recover | Learn/adapt |
|---|---|---|---|---|---|---|
| **Identifying risks** | Vastaamo network had been configured in a way that the data breach could be easily done | Visible patient records / Intranet<br><br>Patient data insufficiently encrypted | Only default password in use<br><br>'Patient register' = may have attracted the attacker | How to prevent blackmail of individual patients or to begin using personal data to commit identity thefts | Information from as many as 2.000 patients visible (28.10.)<br><br>Over 15.000 data breach and ransom case (29.10.) | Patient safety / readiness to see a therapist in the future<br><br>Belief in privacy of treatment |
| **Critical activities** | Some twenty vulnerabilities in server programs to patient register web address | | Network neglected | Vastaamo refuses to pay | Ministry of the interior: victims of data breach need urgent help | Determine if acted according to data protection regulations |
| **Key personnel** | | | | Police be given peace to work | CEO let go / suspected of keeping data breach secret for over a year | Cybersecurity company track where the Bitcoin ransom gone |
| **Guidelines and procedures** | | | Raised need to strengthen cyber security and the level of its control | Paying ransom will not get information back. | Victims need a rapid change of personal identification numbers | Similar companies to Vastaamo will have tighter cyber security requirements |
| **Open communication** | | | Victims informed first only on Vastaamo website (24.10.)<br><br>Data breach reported only weeks after notifying police | Direct ransom demands in Bitcoins<br><br>Victims' first days filled with uncertainty and silence | Clear instructions have only been available during the last day (26.10.) | Data breach ransom demands exceptionally shrewd and showing indifference toward weaker people |

Cyber Threat Intelligence seems to have been neglected in the company. Customer information apparently disappeared already 2018 and 2019. This demonstrates the potential vulnerability of personal data today's information society, and the need for developing cyber security of private healthcare operators. With the help of CTI it would be possible to gain information about possible threats and support the situational awareness and decision making in different stages of resilience.

It seems that identifying risks was also neglected. The Vastaamo network had been configured in a way that the data breach could be easily done, and e.g., the location of patient records and Intranet had been left visible for those who know how to look for them. The title 'Patient register' may have attracted the attacker. Patient data was insufficiently encrypted, and only default passwords in use.

Critical activities overlooked include some twenty vulnerabilities in server programs. The victims needed urgent help which may involve the wider society, and from a legal standpoint it must be determined if the company acted according to data protection regulations. Guidelines and procedures were not enough to ensure the protection of the data. This raises a clear need to strengthen cyber security and the level of control for similar companies.

Communication was not open. The victims were first only informed on the Vastaamo website, and this happened weeks after the police had been notified of the data breach. Once the company refused to pay, the victims began to receive direct ransom demands in Bitcoins. The victims didn't get clear instructions until after a few days. This data breach was deemed exceptionally shrewd as it showed a grave indifference toward weaker people.

## 6. Conclusions

Working in critical sectors is the backbone of society. Strong interconnections highlight vulnerabilities and make it possible for the effect to cascade between organizations. More and more cyber threats target critical infrastructures, threatening their business continuity. When assessing cyber resilience, resilience phases and business continuity management should be combined with cybersecurity processes and principles.

Understanding how functions change in the different stages of resilience can help to quickly detect threats to appropriately counter them for added endurance and stability.

The case of Vastaamo is one indication of how the know-how and professionalism of many companies in the SME sector are not sufficient to develop information security and maintain the continuity of their operations. Data breaches can test a company's ability to continue its operations, and especially sectors critical to society, such as health care, directly affect society's well-being.

Traditional risk assessments and information security management processes do not consider complex interdependencies and their effects on the continuity of operations. By understanding the different stages of resilience, methods can be developed to assess threats, as well as their probabilities and effects on operations. By combining the principles of business continuity with cyber situational awareness created through CTI, the company's resilience can be increased.

Procedures and tools that improve the resilience and continuity of information security could include activities that identify the sector's critical information, functions, and reserves, securely store critical protected information, test the effectiveness of contingency plans and train personnel and stakeholders. Combining the principles of business continuity management and systematic cyber threat assessment can be a way to increase cyber situational awareness, which is needed to support decision-making in all different phases of resilience.

Important topics for further research are the deepening of knowledge and understanding regarding the methods and tools that improve the resilience and continuity of information security mentioned above. Considering the phases of resilience as a reference framework can increase systematicity and the further research and practical development of methods and tools that improve the resilience and continuity of information security.

## Acknowledgements

Acknowledgement is paid to DYNAMO Project, funded by the European Union under grant agreement no. 101069601. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.

## References

Dalal, R.S. *et al.* (2022) 'Organizational science and cybersecurity: abundant opportunities for research at the interface', *Journal of Business & Psychology*, 37(1), pp. 1–29. doi:10.1007/s10869-021-09732-9.

DYNAMO (2022) 'Dynamic Resilience Assessment Method including combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors', Webpage. Available: https://horizon-dynamo.eu/

Edgar, T. and Manz, D. (2017) *Research Methods for Cyber Security*, Cambridge, MA: Elsevier.

Ghafur, S., Grass, E., Jennings, N.R. and Darzi, A., 2019. 'The challenges of cybersecurity in health care: the UK National Health Service as a case study', *The Lancet Digital Health*, *1*(1), pp. e10-e12.

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/

Juntunen, T. (2014) 'Kohti varautumisen ja selviytymisen kulttuuria', *Kriittisiä näkökulmia resilienssiin,* SPEK puheenvuoroja 2, 6-7.

Kotsias, J., Ahmad, A. and Scheepers, R. (2022) 'Adopting and integrating cyber-threat intelligence in a commercial organisation', *European Journal of Information Systems*, pp. 1–17. doi:10.1080/0960085x.2022.2088414.

Lehto, M.; Pöyhönen, J. and Lehto, M. (2019) *Kyberturvallisuus sosiaali- ja terveydenhuollossa, Loppuraportti, Vol. 2,* Jyväskylä: Jyväskylän yliopiston IT-tiedekunta.

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, 407-409.

Linkov, I. and Kott, A. (2018) *Fundamental Concepts of Cyber Resilience: Introduction and Overview*, Cornell University Library, arXiv.org, Ithaca.

Muthuppalaniappan, M. and Stevenson, K. (2021) 'Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health', *International journal for quality in health care : journal of the International Society for Quality in Health Care*, 33(1). doi:10.1093/intqhc/mzaa117.

Munk, S. (2018) 'Interoperability Services Supporting Information Exchange Between Cybersecurity Organisations1'. *AARMS, 17*(3), 131-148.

National Academies of Sciences, Engineering, and Medicine. (2012) *Disaster Resilience: A National Imperative. Washington, DC*, The National Academies Press. https://doi.org/10.17226/13457.

Palma-Oliveira, J.M. and Trump, B.D. (2016) *Modern resilience: Moving without movement, in Resource Guide on Resilience*, EPFL International Risk Governance Center, Lausanne, available at https://www.irgc.org/irgc-resourceguide-on-resilience/

Palomäki, S.; Roschier, S.; Gilbert, Y. and Pokela, P. (2020) *Kestävän tuotannon resilienssi: Kuinka varautua kriiseihin ja kasvaa kestävästi,* Helsinki: Business Finland.

Sedenberg, E. M. and Dempsey, J. X. (31. May 2018) *Cybersecurity Information Sharing Governance Structures: An Ecosystem of Diversity, Trust, and Tradeoffs*, Retrieved 30.3.2019 from https://arxiv.org/abs/1805.12266

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

South Africa Autos Report (2021) *Fitch Solutions Country Industry Reports,* p. 1., Q4 2021.

Turvallisuuskomitea. (2018) *Kyberturvallisuuden sanasto*. Helsinki: Sanastokeskus TSK ry.

Tuttle, H. (2021) 'Ransomware Attackers Turn to Double Extortion', *Risk Management*, vol. 68, no. 2, 2021, pp. 8-9.

Vogus, T.J. and Sutcliffe, K.M. (2007) 'Organizational resilience: towards a theory and research agenda', Paper presented at the *IEEE International Conference on Systems, Man and Cybernetics*.

Whitney, L. (2021) 'Ransomware attackers are now using triple extortion tactics', *Tech Republic*, May 12, 2021.https://www.techrepublic.com/article/ransomware-attackers-are-now-using-triple-extortion-tactics/

Yin, R. (2009). *Case study research: Design and methods* (Ed. 4), Thousand Oaks: Sage.