CASE STUDY

Annals of Disaster Risk Sciences

Vol 3, No 1 (2020): Special issue on cyber-security of critical infrastructure

Business Continuity for Critical Infrastructure Operators

Harri Ruoslahti, Laurea University of Applied Sciences

Address for correspondence: Harri Ruoslahti, Laurea University of Applied Sciences, Finland, e-mail: harri.ruoslahti@laurea.fi

Abstract

Critical infrastructures often lack resilience and easily lose critical functionalities if hit by adverse events. Continuity management strategies for critical infrastructure operators and the networks that they form, rely also on the functionality of other interrelated networks. Disruptions in operations may affect society and for this reason, securing the operations of critical infrastructure operators is important. The technological impacts of CPS become evident to the resilience of all fields of critical infrastructure, but there is also human elements to take into account. The research question of this study is: How to enhance business continuity of critical infrastructure? This case study research uses qualitative methods collected by conducting interviews of resilience and continuity professionals who work with Finnish critical infrastructure. Resilience and continuity management are key for critical infrastructure operators. Important factors identified were identifying risks, critical activities, key personnel, creating guidelines and procedures, and open communication, which themes were recognised as important to improve resilience and manage continuity.

Keywords

Business Continuity, Critical Infrastructure, Risk assessment, Impact analysis

1. Introduction

Critical infrastructures (e.g. transportation, communications, finance, energy, food and water supply) of society may lack resilience (Ruoslahti, Rajamäki & Koski, 2019), and easily lose critical functionalities when hit by an adverse event (Linkov et al., 2014). One practical example of an adverse event is the ransomware attack on the city of Baltimore that disrupted its critical services for weeks. City officials were forced to implement manual procedures to handle critical functions, e.g. real estate transactions, utility payments, property taxes. Baltimore spent more than $18 million on its recovery efforts (Fortinet, 2019).

Continuity management strategies for critical infrastructure operators and their networks, may rely on the functionality of other interrelated networks, and these can be considered being part of a system constituting of systems – a system of systems. Thus, resilience and continuity can be enhanced by the study and improvement of interconnectivity between these relevant networks (Linkov et al., 2014). Enhancing the social networks that surround an organization can also be seen as an important component of societal resilience (O'Rourke, 2007). While risks in collaboration among networks can be reduced, they cannot be avoided. Thus, organizational resilience provides tools and conditions to mitigate crises by understanding and reducing risks (Vos, 2017), and resilience and continuity build on situational intelligence (Pirinen, 2017).

Continuity of operations become enhanced, when different actors, such as authorities, have interoperability and capability to supplement and, when needed fill in for each other (Tikanmäki & Ruoslahti, 2017; Ruoslahti & Hyttinen, 2016). Co-creation results from complex interactions and it may result in resource integration among the many network actors (Pinho, et al., 2014), while also non-hierarchical interaction helps solve a common problem with other stakeholders (Roloff, 2008). Network operations benefit from a common aim (Ruoslahti, 2017), but network actors also need to be aware of having different interests (Vos, 2018).

The research question of this study is: How to enhance business continuity of critical infrastructure?

2. Resilience and Business Continuity

Service disruptions and cyber-attacks against essential systems and networks are on the rise (Pahi, Leitner and Skopik, 2017). Disruptions in operations may affect society as a whole, and for this reason securing the operations of critical infrastructure operators, public or private, may be crucial for a functioning society (Ruoslahti, Rajamäki & Koski, 2018). The Network and Information Security (NIS) Directive of the European Union (EU) (European Commission, 2016) strongly calls for Public Private Partnership (PPP), collaboration between authorities and the private sector, in the critical field of cyber security. Continuity of operations can be enhanced with collaboration between the different actors (e.g. authorities and industry), and having interoperability and capabilities to supplement and even fill in for each other (Tikanmäki & Ruoslahti, 2017; Ruoslahti & Hyttinen, 2016).

Complex interactions, and even resource integration to enhance resilience and continuity among the many network actors may ultimately result in co-creation (Pinho, et al., 2014), where common aims (Ruoslahti, 2018), and non-hierarchical interaction with other stakeholders also help solve common problems (Roloff, 2008). Vos (2017) proposes that risks in co-creation and collaboration networks can be reduced, but not totally avoided, and that organizational resilience provides tools and conditions to understand and reduce risks, and to mitigate crises. Resilience thus, requires collaboration by and between social networks, where communication becomes co-constructed through the various interactions between the multiple stakeholders, who participate in it. Network stakeholders may very likely have different interests and various other interdependencies to contend with (Vos, 2017). Co-creation requires interaction among various actors who need knowledge creation processes to build resilience in their networks, while also guiding connected stakeholder networks to do the likewise (Gustafsson, Kristensson and Witell, 2012). The roles, engagement, and responsibility of these actors, their mutual interactions, and impacts become key factors in network collaboration, while situational intelligence is also needed when building resilience (Pirinen, 2017).

Many of today's systems include complex interconnections and linear and non-linear relationships between multiple subsystems, which are both social and technical. Systems that combine both social and technical elements are considered sociotechnical systems (Singapore-ETH Centre, 2015), or cyber-physical systems (CPS), demonstrating seamless integration between computational, human and physical elements. These are subsets of sociotechnical systems (Broy & Geisberger, 2011). According to Murakami (2012) cyber-physical systems include inputs and outputs between cyber, physical, and social worlds, where computational elements interact with technical, ecological elements, organisational, and human elements, by using cyber networks and the Internet, and by the design of and to the benefit of society CPS are rapidly transforming the ways in which we interact with the physical world. Thus, the technological impacts of CPS become evident to the resilience of all fields of critical infrastructure; e.g. engineering resilience (Levenson et al., 2006), disaster management (Dahlberg, et al., 2015) and healthcare (Rajamäki & Pirinen, 2017). Many critical infrastructures of our society may thus, lose their critical functionalities when hit by adverse events (Linkov et al., 2014). Amir and Kant (2018) note that sociotechnical systems are intentional hybrids of people and technologies. They involve complex interactions between people, organizations and technologies, and their complexity complicate their resilience. According to Ruoslahti, et al. (2018) most CPS are complex and interconnected and for this reason the experiences and characteristics from multiple sectors of critical infrastructure should be considered simultaneously.

The National Academy of Sciences (2012) identify four resilience event management cycles. The first is phase is Plan, during which plans and preparations to keep services available are made. The second phase Absorb aims to isolate and maintain the most critical assets, functions and services, while the occurring disruption is being repelled. The third phase Recover seeks to restore the availability of all services. The final phase Adapt is about learning from the experiences and modifying resuming operations to be more resilient against future events (National Research Council, 2012).

Ruoslahti, et al. (2018) find that CPS education should cover all event management cycles (plan or prepare, absorb, recover, adapt and learn, and self-modify) and resilience domains (physical, information, cognitive and social). The management strategies for critical infrastructure networks (e.g., telecommunications, electricity, or transportation) often rely also on the functionality of interrelated networks, which together can be considered systems of systems. Resilience can thus, be enhanced by the study and improvement of the interconnectivity of these relevant networks (Linkov et al., 2014), and by enhancing the surrounding social networks, which also are important for increased societal resilience (O'Rourke & Briggs, 2007). The preparation phase creates a basis for the ability to absorb and recover from a disruptive incident, after which the adaptation phase creates a feedback loop that enhances future preparation phases; a cyclical process, as is Business Continuity Planning (BCP) (Savage, 2002). In addition, other classifications, such as the four domains by the Network-Centric Warfare (NCW) doctrine (Alberts, 2002) 1) physical, 2) information, 3) cognitive, and 4) social, may help create shared situational awareness and act as basis for decentralized decision-making. CPS possess both physical elements, where information is stored and processed to provide a basis for cognitive decisions by the systems users and the social level its multiple stakeholders.

Open collaboration benefits the aims of all critical infrastructure network stakeholders seeking for resilience. Open innovation environments, such as the Common Information Sharing Environment (CISE) and the Finnish disruption service management network (KRIVAT), are prime examples of CPS frameworks that actively facilitate interaction between network stakeholders. (Ruoslahti, et al., 2018). On a European level project ECHO – European network of Cybersecurity centres and competence Hub for innovation and Operations – aims to establish a coordinated network of cyber security specialists and service providers to, through effective and efficient multi-sector collaboration, proactively strengthen cyber security in the European Union (Rajamäki, Tikanmäki & Räsänen, 2019). Pöyhönen et al. (2020) argue that integrating a view of three levels of organizational decision-making to the five-layer cyber structure by Lehto & Neittaanmäki (2018) a more comprehensive system view of the cyber security environment of organizations and systems can be gained. In addition they find that The Observe – Orient – Decide - Act (OODA) loop, can, as a framework, provide structure to the collaboration aiming to better Cyber Situational Awareness (CSA). The OODA loop is used e.g. in project ECHO (ECHO, 2019) and other cyber security decision-making (Pöyhönen et al., 2020).

When a threat meets a vulnerability and a capability to cause a consequence, it may be considered a risk (Linkov et al., 2014). Crisis management aims at organizations to sustain and resume their operations, minimize financial losses to stakeholders, and learn to better manage future incidents (Pearson & Clair, 1998). The Finnish KRIVAT concept involves organizations from various sectors of critical services who, when encountering disturbances or crisis, share information and take needed actions together. Thus, critical infrastructure operators and their support organizations have a shared system for real-time information exchange between these organizations when incidents occur.

Ruoslahti (2019) finds that the structure of input, throughput and output communication (Vos & Schoemaker, 2004) is one useful framework to make sense of communication in a networked process of co-creating knowledge. Forms of input communication may include use cases and scenarios. Throughput communication concerns the collaborative work among internal and outside stakeholders. Output communication includes communicating about the aims, work and results to staff, stakeholders and wider audiences.

3. Method

This case study (Yin, 2003) research uses qualitative methods that are collected by conducting interviews and observing interactions (Denzin and Lincoln 1994). The research by Baskerville and Myers (2009) suggests that

"academic work is usually synchronous with practitioner interests" (p. 648). This research and its research question (How can business continuity of critical infrastructure be enhanced?) focuses on practitioner interests using an academic approach. Masters students contributed the practical collection of the sample data, which are based on 22 interviews of Finnish resilience and continuity professionals, conducted during the spring term of 2018, as part of their studies in Continuity management. In line with the demands of research ethics, each interviewee was asked for informed consent before the start of each interview.

The cross-case analysis of this data was conducted by the author in late 2019. The analysis is based on first narrowing the sample to exclude a Data Extraction Table (DET), designed, based on the research question, specifically for this study. The themes that emerged from the sample data are presented in the Results section and discussed further in the Conclusions section.

4. Results

According to the interviews resilience and Business Continuity Planning (BCP) is required by law and according to the national security and cyber-security strategies for large governmental organisations, which have long traditions in securing their operations against disruptive incidents.

Identify Risks

Respondents noted that most important is to identify risks. This should be elaborated by estimating the effects of disruptions by performing a Business Impact Analysis (BIA) and determine Recovery Time Objective (RTO) and Recovery Point Objective (RPO). All these serve as basis for the availability of functions and services.

Results indicate that risks can be on two levels: strategic and operative. On a strategic level can be serious disruptions in power and utilities, IT-infrastructure or serious cyber threats. On an operative level are the risks related to one's own processes and especially one's IT-processes, plus human related risks, such as faulty change management or risks related to key personnel.

Many disruptions however are technological, such as cyber risks, or those related the physical environment (e.g. data communications and power and water distribution). In addition, risks that are related to personnel skills should be taken into account. Some most probable threats against critical infrastructure were mentioned to be those against their information technology.

One noted problem when operations are being changed or new operations begun, are the unidentified risks. Resilience was named as a way to prepare for the unexpected. Acute situations call for quick adaptability.

Critical Activities

Identifying the critical activities are important in business continuity management and mitigating disruptions. Different risk management tools can be used when planning for business continuity.

To get over disruptions, day-to-day operations are best built on a strong base. Operations and personnel are concentrated in existing sites during disruptions. Respondents note that critical functionalities should be identified, and responsibilities to keep these critical operations determined; focus on core functions.

Exercise is key, and though this may interfere with daily operations, management support and participation are needed, note respondents, as well as that training and exercise are embedded in organisational culture. Results indicate that successful security management is best based on identifying risks and a holistic approach to security.

One quoted example case stressed the importance of the continuity of IT-operations was a food production company that receives some 95 % of all its approximately 100.000 daily orders electronically. These orders it must fulfil in 36 hours. Any disruptions will then have direct effects to other actors further down on the critical food supply chain.

Key Personnel

The availability of key resources is key for continuity. Competences for action are important for successful crisis management. These competences include the ability to collaborate with other employees and stakeholders, and the ability for situational awareness, which focus on what one can influence and if the problem needs to be escalated further.

Besides guidelines, training is key for people to be able to perform during crisis situations. Identifying key personnel is, according to interviewees, one important element, when improving resilience. One way of improving resilience is that important information is accessible and shared between several people, and not known by just one person in the organization.

Respondents stressed the availability of skills and competences during disruptions. This was noted as especially important in relation to IT-systems – these systems need competent users or the situation may even become worse. Building competence networks ahead of time was noted as one way to prepare for this.

Guidelines and Procedures

The results stress the importance of clear roles and responsibilities for encountering different situations, and to ensure proper procedures. Guidelines and procedures should be tested and practiced before disruptions strike. Results indicate that successful continuity management should be continuous and systematic. The ISO-standard PDCA (Plan, Do, Check, Act) –principle was mentioned as one approach that may promote a systematic approach. Thus, continuity planning calls for updating and testing of procedures and networks in real-time.

Requirements for the IT-systems of critical infrastructure and their cyber security should be made in relation to the service that it provides, and it was noted that all partners should have the skills and competences to plan and prepare. Regularity and schedules were also stressed in continuity management, as was leadership. Continuity management needs to be kept on the agenda.

Open Communication

Respondents note that continuity requires human interaction and communication and this calls for regular contacts and all parties having a willingness to collaborate and solve problems together. Thus, one critical element of continuity management that the results show is communication. Open communication was seen as a way to promote resilience, and results also show that it is important to raise awareness toward better collaboration between the many critical infrastructure actors.

Results show that holistic and collaborative approaches from all value chain and network participants and engaging people of their organisations can facilitate identifying risks.

According to the respondents, anomalies and disruptions must be observed and efficient counter measures instigated together with stakeholders. This calls for plans that have been tested through regular exercises. The choices of which services need to be restored first should be made beforehand to secure needed resources and critical situations often call for having optional procedures.

5. Conclusions

Resilience and continuity are key for critical infrastructure operators. Some important factors are a) identifying risks, b) critical activities, and c) key personnel, as were d) guidelines and procedures, and e) open communication. These themes (see table 1) were recognised as important, when improving resilience and managing continuity. Recognising the role of these elements can help the critical infrastructure operators structure and guide their business continuity planning processes, and focus on co-creative collaboration towards improved resilience and a more resilient society.

Table 1. Themes important for improving resilience and managing continuity

	Plan	Absorb	Recover	Adapt
Identifying risks	Identify risks and their impacts	Plans to action	Ease recovery	Learn, make new plans, re-identify risks
Critical activities	Identify critical activities, RTO, RPO	Focus on critical activities according to RTO, RPO	Resume more and more functionality, towards normal	Improve processes and functions, new RTO, RPO
Key personnel	Identify key people and skills, exercise	Have needed skills available	Broaden involved people and skills	Revise list of key people and skills
Guidelines and procedures	Create guidelines and procedures	Improvise, but follow if possible	Less improvisation, more procedures	Revise guidelines and procedures
Open communication	Share plans with networks and engage personnel	Share information with network and engage personnel	Collaborate with network and engage personnel	Collaborate in making new plans, engage personnel

Identifying risks, and many of these are technological, is thus, be seen as a starting point. Then identifying critical activities and the services that absolutely must first recover becomes key for business continuity management and mitigating possible disruptions to critical infrastructure.

Exercise, as well as a holistic approach to security, and the availability of key resources, skills and competences become key for continuity management, while engaging people to clear roles and responsibilities and collaborative approaches from all stakeholders provide a basis for open communication and co-creation.

The results indicate that the respondents have read their business continuity management and planning literature, as much of the results seem to support the views gained from literature. Being resilient and prepared was seen important. Co-creative collaboration and sharing of information was seen important, especially when absorbing and recovering from possible disruptive incidents. This research thus, contributes to resilience theory and also has very practical implications for critical infrastructure operators.

Acknowledgement

This work was supported by project ECHO, which has received funding from Horizon 2020 research and innovation programme of the European Union under the grant agreement no. 830943. The European Commission funds cyber pilot projects like the European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO) to promote opportunities for researchers, solution providers and practitioners to study and co-create new knowledge for innovation from multiple perspectives.

References

Alberts, D. (2002). Information age transformation, getting to a 21st century military, Defense Technical Information Center, Fort Belvoir.

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

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

Broy, M & 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.

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

ECHO - the European network of Cybersecurity centres and competence Hub for innovation and Operations (2019). ECHO Website, [Online] Available at: https://echonetwork.eu/project-summary/ [Accessed December 8 2019]

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 [Accessed June 8 2019].

Fortinet (2019). Fortinet Q2 2019 Quarterly Threat Landscape Report, Fortinet, Inc.

Gustafsson, A, Kristensson, P, & Witell, L. (2012). Customer co-creation in service innovation: a matter of communication?, Journal of Service Management, Vol. 23 No. 3, 2012 pp. 311-327.

Lehto, M. & Neittaanmäki, P. (2018). The modern strategies in the cyber warfare. Cyber Security: Cyber power and technology. Berlin: Springer.

Linkov, I et al. (2014). Changing the resilience paradigm, Nature Climate Change, Vol 4, pp 407– 409.

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.

National Research Council (2012). Disaster Resilience: A National Imperative, The National Academies Press, Washington, DC.

O'Rourke, T. D. & Briggs, T. R. (2007). Critical Infrastructure, Interdependencies, and Resilience. The Bridge, Volume 37.

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

Leveson, N., Dulac, N., Zipkin, D., Cutcher-Gershenfeld, J., Carroll, J., & Barrett, B. (2006). Engineering resilience into safety-critical systems. Resilience engineering: Concepts and precepts, 95-123.

Pearson, C & Clair, J. (1998). Reframing Crisis Management, Academy of Management Review, Vol 23, No. 1, pp 59–76.

Pinho, N, Beirão, G, Patrício, L & Fisk, R. (2014). Understanding value co-creation in complex services with many actors, Journal of Service Management, vol. 25, no. 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, 259 -266.

Pöyhönen, J., Rajamäki, J., Ruoslahti, H. & Lehto, M. (2020). Cyber Situational Awareness in Critical Infrastructure Protection. Presented at CYSEC 2020: Cyber Security of Critical Infrastructure, April 28 – 30, Dubrovnik, Croatia.

Rajamäki, J & Pirinen, R. (2017). Design science research towards resilient cyber-physical eHealth systems, Finnish Journal of eHealth and eWelfare, Vol 9, No. 2–3, pp 203–216.

Roloff, J. (2008). Learning from Multi-Stakeholder Networks: Issue-Focused Stakeholder Management', Journal of Business Ethics, 82:233–250.

Ruoslahti, H. (2019). Co-creation of knowledge for innovation in multi-stakeholder projects. JYU dissertations.

Ruoslahti, H. (2018). Co-creation of Knowledge for Innovation Requires Multi-Stakeholder Public Relations, in Sarah Bowman , Adrian Crookes, Stefania Romenti, Øyvind Ihlen (ed.) Public Relations and the Power of Creativity (Advances in Public Relations and Communication Management, Volume (3) Emerald Publishing Limited, pp.115 - 133

Ruoslahti, H & 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. & Koski, E. (2018). Educational competences with regard to resilience of critical infrastructure. Journal of Information Warfare. Journal of Information Warfare 17.3: 1-16.

Savage, M. (2002). Business continuity planning', Work Study, Vol 51, No. 5, pp 254–261.

Singapore-ETH Centre (2015). Future Resilient Systems, [Online], https://www.ethz.ch/content/dam/ethz/special-interest/dual/frs-dam/documents/FRS-Booklet.pdf.

Tikanmäki, I. & Ruoslahti, H. (2017). Increasing Cooperation between the European Maritime Domain Authorities, International Journal of Environmental Science, Vol 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.

Vos M. & Schoemaker, H. (2004). Accountability of Communication Management, A Balanced Scorecard for Communication Quality, Lemma Publishers, Utrecht, 2004.