5-11-2023

PREPARING FOR CYBERATTACKS: A CASE STUDY OF RESILIENCE IN THE HEALTH-CARE SECTOR

Manuel Weber
University of Liechtenstein, manuel.weber@uni.li

Janine Hacker
University of Liechtenstein, janine.hacker@uni.li

Laura Karintaus
Tampere University, laura.karintaus@tuni.fi

Samuli Pekkola
Tampere University, samuli.pekkola@tuni.fi

Jan vom Brocke
University of Liechtenstein

See next page for additional authors

PREPARING FOR CYBERATTACKS: A CASE STUDY OF RESILIENCE IN THE HEALTH-CARE SECTOR

Research Paper

Manuel Weber, University of Liechtenstein, Vaduz, Liechtenstein

Janine Hacker, University of Liechtenstein, Vaduz, Liechtenstein

Laura Karintaus, Tampere University, Tampere, Finland

Samuli Pekkola, Tampere University, Tampere, Finland

Jan vom Brocke, University of Liechtenstein, Vaduz, Liechtenstein

Maija Ylinen, Tampere University, Tampere, Finland

Abstract

Nowadays, health-care organizations rely extensively on information technology and systems for providing high-quality services to their patients and exchanging data with external partners. However, these organizations, processes, and operations are vulnerable to criminal activities and digital security breaches, which has led health-care organizations to build various protection mechanisms, including firewalls, virus scanners, and security policies that enhance their ability to prepare for threats; design activities to be conducted during a cyberattack; and implement means to recover from an unfortunate event. Although these moves have been acknowledged in research and in practice, there is still little knowledge available on how organizations understand and perceive such events as well as their consequences. To this end, we conducted a qualitative case study that included 14 interviews with diverse key actors at a Finnish hospital. From them, we aimed to understand how the organization has prepared for cyberattack resilience. By generalizing our case research, we built a framework for analyzing and improving organizational resilience. This framework makes significant contributions both to theory and practice.

Keywords: Health-Care Organizations, Cyberattacks, Resilience, Qualitative Case Study.

1 Introduction

Health-care organizations utilize information technology (IT) to optimize their processes, share data, and better analyze and process their patients' medical data. This trend not only provides opportunities and the potential to further expand high-quality medical services and treatments but also entails risks. Cybercrime and attacks emerge, taking different forms and having a variety of consequences for organizations and society (Boddy et al., 2017; Jeffcott et al., 2009; Safavi et al., 2018).

Generally speaking, it is challenging to get all people and departments within an organization "on the same page" (Rajivan and Cooke, 2017). Concerning cyberattacks, the biggest challenge for any organization is to prepare for an event (i.e., a cyberattack) without knowing or being able to estimate when a security breach might take place, what form it will take, and the kind of consequences it will have. The situation is exacerbated in hospitals, where professionals with different expertise, awareness, and focus must work together. Since health-care personnel use various forms of IT to carry out their tasks, the danger of cyberattacks can quickly threaten patients' health. Also, many devices are connected to the Internet, exchanging data with other systems and equipping health-care personnel with vital information for diagnosing and treating patients, which adds another layer of risk. This could be fatal if

ventilators or automated medicine dispensers, for example, which determine whether a person lives or dies, are placed under a cyberattack (Coventry and Branley, 2018).

The topic is little studied. Rare examples of research include studies of simulated attacks, such as using drones to conduct wireless attacks. Still, these studies have focused on technical vulnerabilities and protection (Sethuraman et al., 2020). In contrast, limited knowledge is available for understanding the managerial measures and activities that health-care organizations perform to prepare for cyberattacks at the organizational level. We thus aim to understand how organizations that are heavily dependent on the use and integration of IT (i.e., health-care organizations that save people's lives) deal with cyberattacks. More specifically, we aim to generate knowledge on how to prepare for such adverse events and how stakeholders and human actors can carry out mitigating measures. In doing so, we seek to discover how these measures are not merely superficial but constitute an integral part of health-care employees' work practices. We go on to briefly discuss the existing and preliminary research to demonstrate the research gap. The absence of theoretical knowledge and the topic's current relevance lead us to the following research question: *How can organizations prepare for cyberattacks and achieve resilience at the organizational level?*

We propose an empirically grounded framework and guidelines for achieving shared understanding as a building block for organizational resilience. These guidelines help practitioners to achieve organizational resilience in the face of different cyber threats, and perhaps when they are faced by any other type of threat. The results demonstrate the need to integrate the possible threats and the negative consequences of cyberattacks, not only within the collective mind of an organization but also in the successful integration and design of organizational structures, processes, and practices. For example, our case hospital needed to align the awareness of all key actors and employees from strategic and operational points of view. These shortcomings, once identified and acknowledged, will help organizations to advance their organizational resilience. In this regard, we better understand how to prepare for such events at the corporate level while considering different roles and responsibilities within one single organization associated with conscious and unconscious preparation for cyberattacks. As a result, we develop a framework for analyzing and improving organizational resilience dedicated to cyberattacks.

The paper is organized as follows. Following this introduction, we present the related research and discuss the concept of resilience. We then present the overall research design and the methodologies applied. Finally, we discuss our results and conclude with final remarks.

2 Related Research and Research Background

In this section, we provide a brief overview of the seminal works that have studied resilience in the health-care context. We also elaborate on this multi-faceted concept and provide a short overview of how the term is generally used within the scholarly community.

For years, resilience has gained broad interest as the implications of various disruptions or negative events on ecosystems, communities, organizations, or processes have become evident. Scholars are especially interested in understanding the dynamics (Burnard and Bhamra, 2011) and how organizations can deal with adverse events or survive in turbulent environments. However, the concept and its definition lack clarity and are even ambiguous. Each discipline has its ontology and applies different methods and tools (Hillmann, 2021; Hillmann and Guenther, 2021). Within the management and business science literature in particular, scholars have applied different theoretical lenses and used the term resilience differently (Bhamra et al., 2011a; Linnenluecke, 2017). Whereas some scholars have depended on agency theory (e.g., Sarkar et al., 2017), others have relied on resources theory (Wang et al., 2019) or deployed the broaden-and-build theory of positive emotions (Kohn, 2020). As a result, various conceptual frameworks have been developed (e.g., Maruyama *et al.*, 2014; Weber, Hacker and Vom Brocke, 2021).

Over the last decade, the notion and concept of resilience has been examined on several levels, such as in the study of Bhamra, Dani and Burnard (2011b). Välikangas and Romme (2012), for example, saw

readiness for change as a prerequisite for an organization's resilience. To this end, they referred to the concept of operational resilience, which is the ability to respond (e.g., recover) after adversity, and strategic resilience, which is the ability to turn any type of adversity into an opportunity. Hence, they saw operational resilience as recovery-based and strategic resilience as renewal-based. Similarly, Wieland and Wallenburg (2013) conceptualized resilience as a function of two dimensions—while agility is denoted as the reactive component, robustness is perceived as the proactive part (Braunscheidel and Suresh, 2009; Shukla et al., 2011). Burnard and Bhamra (2011) provided the following extensive definition for organizational resilience: "*Resilience is the emergent property of organizational systems that relates to the inherent and adaptive qualities and capabilities that enable an organizations adaptive capacity during turbulent periods. The mechanisms of organizational resilience thereby strive to improve an organization's situational awareness, reduce organizational vulnerabilities to systemic risk environments and restore efficacy following the events of a disruption*" (p. 5587). Berg et al. (2018) provided an integrative view of resilience in health-care research and different methodological strategies.

These studies primarily focused on the individual level, whereas research at the organizational level remains somewhat limited. Nevertheless, the literature advocates that resilience is a multi-level construct that needs to be studied at the micro, meso, and macro levels. One such broad example was provided by Jeffcott et al. (2009), who offered a systematic and holistic conceptualization of resilience in the health-care context, focusing mainly on clinical handovers, which give patient safety a high priority (e.g., Jeffcott et al., 2009; Pedersen, 2016; Rangachari and Woods, 2020).

Similarly, we found existing resilience studies in the context of health-care organizations. The majority of these applied a purely technical perspective and discussed topics such as data availability, data security, protection measures, or the adoption of IT to prepare organizations from cyberattacks (Boudko and Abie, 2019; e.g., Coventry and Branley, 2018; Kelli et al., 2021; Safavi et al., 2018; Zhang et al., 2020). Other studies have investigated how human actors deploy IT to prevent cyberattacks and thus applied a socio-technical lens (Nifakos et al., 2021; e.g., Rajamäki and Pirinen, 2017). Boddy et al. (2017), for example, studied data behavior and analytics and visualization. The studies agree that data and application safety is paramount. The increased connectivity of medical devices among health-care (clinical) enterprises and the exchange of data across enterprise boundaries has become an ever more frequent target of criminal activity (Bhosale et al., 2021; Coventry and Branley, 2018; Sood and Moidu, 2018). Related work in this area has also investigated the application of different types of IT, such as IoT (e.g., Boudko and Abie, 2019; Zhang et al., 2020), blockchain (Kelli *et al.*, 2021; Safavi *et al.*, 2018), and machine learning (e.g., Boddy et al., 2017; Kelli et al., 2021). Other studies have explored using AI, big data, and IoT to create a digital twin and protect that data (Zhang and Tai, 2022). Coventry and Branley (2018) provided another technical perspective when they discussed the use and connectivity of electronic health-care technology. Such technology, on the one hand, creates benefits for patients and care delivery but, on the other hand, is vulnerable to cybersecurity breaches or attacks and thus can have serious health consequences. The authors advocated that cybersecurity must become integral to patient safety and the patient care culture. Along these lines, Nifakos et al. (2021) examined human factors that influence resilience. They adopted a socio-technical perspective and investigated the need for and role of awareness and training programs and related cyber security activities that are provided to health-care employees. They also conducted a systematic literature review to understand the role of health-care staff in such programs and training activities. They reviewed the assessment methodologies and strategies that organizations adopt to counteract cybersecurity risks and attacks, concluding that collaboration and standardization in these programs and information and awareness campaigns are critical factors for strengthening organizations' awareness of cyber security issues.

Along the same lines, Rajamäki and Pirinen (2017) studied how cyber security in health-care infrastructure has evolved over the years. They addressed current cyber security challenges, such as system availability, access control and authentication, network security, and socio-technical aspects, and proposed design principles to increase systems' resilience toward cyberattacks.

Organizations prepare for cyberattacks by using various means. However, the existing research focuses on technical issues; that is, how technologies can be secured, not how organizations' resilience can be improved. Addressing this gap, we examine organizational resilience to cyberattacks in the context of health-care organizations (Siponen and Oinas-Kukkonen, 2007). We do this by conducting an in-depth qualitative case study with a multi-stakeholder perspective, which we describe in the following section.

3 Research Design and Methods

3.1 Research Design and Context

We adopted a research design with a single and qualitative case study (Eisenhardt, 1989). In general, case studies enable an understanding of organizational behavior and then generalize the results to other contexts. This research design allowed us to study the interviewees' rationale for their managerial decisions and to elaborate on their experiences with cyberattacks. In this single and non-comparative case study (Thomas, 2011), we were able to collect in-depth responses from interviewees from different departments and with different experiences.

We conducted our study at a large government-funded hospital in Finland (Europe). The hospital operates in all possible areas of care, including acute and non-urgent care; performs all kinds of surgeries and cancer treatment; and has a maternity ward and psychiatry department, among many other facilities. The hospital has over 1000 beds and 6000 employees, and it cares for more than 250,000 patients annually. Different operations are divided into various departments, each managed as an independent unit (team) and/or subsidiary and led by a managing director. In the hospital, the supreme decision-making power is located in the hospital council, which selects a board responsible for managing operations. Under the board is the corporate governance, which is led by the director of the hospital district. The care operations of the hospital district are again led by a chief physician.

The hospital's IT operations are organized under a centralized IT department that manages systems development, strategic issues and policies, and user training, and an outsourced IT-partner is responsible for keeping the systems running. The internal IT department is in daily contact with partner organizations. Together, they are responsible for how the hospital operationally attempts to secure itself against potential cyberattacks, with the IT partner managing the technology and the IT department responsible for coordination and social issues.

3.2 Data Collection and Analysis

We collected qualitative data by interviewing relevant stakeholders involved in and impacted by potential cyberattacks. Between April and August 2021, we interviewed 14 employees at the hospital to gain their assessment of how well prepared they were for cyberattacks and what measures they had taken in their organization.

A semi-structured interview protocol provided structure through a set of pre-defined open questions and flexibility in accounting for different experiences with cyberattacks or different areas of knowledge, which we were able to deepen (Murray, 2018; Roulston and Choi, 2018). In total, three researchers (authors; junior, advanced, and senior) were involved in the process of data collection and analysis. Collectively, they prepared the interview questions, which are attached in the Appendix. To gather domain and contextual knowledge, the junior scholar conducted two meetings with each of the IT department representatives. The insights from these enhanced the scholars' understanding and later assessment of the findings. After these preparatory measures, the junior author conducted the interviews, which were audio-recorded using Microsoft Teams and later transcribed. Another scholar (advanced) supported and advised the junior scientist during the data collection process. To make sense of the responses and structure them accordingly, the findings went on to be discussed among all three scholars (Pekkola et al., 2019). Table 1 shows an excerpt of two sample quotes, with only the illustrative quotes translated from Finnish. The table also illustrates how we evaluated qualitative responses.

Quote	Themes	Groupings (generalized from all interviews)
There has been no external resilience assessment nor training. We know [cyberattacks] exist and may occur. It would be good to prepare for them and have some training. We have done so with other crises and perils. (Nurse)	Cyberattack resilience has not been assessed. Identifying the cyberattack risk. No training for cyberattacks. Training on other exceptional situations.	No organization-wide assessment of cyberattack resilience. Cyberattack risk to be identified. Not everybody has had training for cyberattacks. There is more training for other situations than for cyberattacks.
Alternative work practices should be internalized, and we should not rely on information systems too much. In every unit, there should be a clear plan when [the word 'when' was used instead of 'if'] something happens. I'm very proud that we [my unit] are prepared. Every process has been thought through from the beginning. Others might not have as good a situation. (Care manager and coordinator E)	Comprehensive work practices for exceptions are internalized in advance so that everyone knows how to act. Strong trust toward the unit's preparedness plan. Uncertainty about the departments in the hospital.	The plans are department specific. Well-defined and specified plans exist. Uncertainty of whether the whole hospital is prepared for a cyberattack and if all staff know what to do if an attack occurs.

Table 1. Interview quotes, translated from Finnish.

In total, we conducted 14 interviews, each lasting 63 minutes on average. The participants were selected using a snowballing technique from the four departments that would be significantly impacted in the case of a cyberattack. The interviews began with the IT department, which provided us with contact persons from the respective departments, after which the interviewees were asked to suggest additional interviewees. The interviewees included IT department personnel (five people: IT management, IT security, and medical IT), general management (two people: public relations and communications and management of operational activities), and selected health-care personnel representatives (seven people: nurses, physicians, and unit managers in four departments, namely the emergency, imaging, and surgical departments and the maternity ward). These four departments provided an illustrative example of the hospital's operations; some other departments, such as the cafeteria or facility management, would only be affected secondarily.

At first, we interviewed the IT department representatives responsible for cyberattack preparedness in the hospital and for related policies, instructions, and training materials as well as the general managers who would manage potential cyberattacks. From there, we moved our focus to health-care personnel for whom the day-to-day activities of cyberattack prevention were more distant but on whose work a cyberattack would have a significant effect. We did not interview the IT partner due to its sole focus on technology and technology management.

Following an interpretive approach, the data analysis proceeded inductively from audio file transcripts (Walsham, 2006, 1995). Reoccurring themes were initially identified, and similar themes were grouped. We then visualized a plot and developed a process diagram (Figure 1) to understand and conceptualize how the organization reacted to cyberattacks. In the following section, we begin by providing background on how the interviewees conceptualized cyberattacks and then present the themes regarding preparation for cyberattacks and the challenges linked to the current preparation processes in the case hospital.

4 Findings

4.1 Types of Cyberattack

We asked the interview participants to identify a "typical" cyberattack. The interviewees' comprehended the notion very differently, with some very knowledgeable and others having very little understanding of it. Possible cyberattacks included denial of the service attacks on different servers and other attacks that would prevent the use of information systems (IS) or other technologies. The scenario that received most speculation focused on inoperable systems. For example, a cyberattack on, or even a small interruption affecting, respirators, pacemakers, and other nursing equipment could be fatal (Health-care personnel, D, H), especially if multiple items of equipment were attacked simultaneously. An attack on the electronic access control would be problematic, since people could either be locked out on the wrong side of the door or the doors would fully open, allowing anyone to enter (Health-care personnel, B).

Table 2 summarizes the interviewees' understanding of a typical cyberattack. All interviewees mentioned the first three types quite commonly, but the fourth type (i.e., IoT attacks) was only mentioned by the medical IT staff and aggregated by the IT people.

Type	Possible consequences
Denial of the service	- Haste, bottlenecks - Patient safety risks - Reputation problems, economic issues
Information theft, data leakage	- Problems related to individual patients - Reputation problems, economic issues
Modifying the data	- Significant patient safety risks - Haste, bottlenecks - Reputation problems, economic issues
Attack against medical devices (IoT)	- Significant patient safety risk - Reputation problems, economic issues
Aggregate (cyberattack + catastrophe)	- Patient safety risks - Haste, bottlenecks - Reputation problems, economic issues

Table 2. Summary of the interviewees' understanding of cyberattacks (own illustration).

The interviewees were quite unanimous about the severity of cyberattacks. In hospitals, the risks were seen to be broader than "just" the loss of profits or business discontinuity, since they might threaten human lives. The most prominent risk was the threat to patient safety. The interviewees agreed that minimizing such threats should be an everyday practice, since any disruption can always be fatal.

If a cyberattack were to inactivate IS, new needs would quickly emerge. For example, in a normal situation, patient record systems are regularly used to check medical histories (e.g., diagnoses, operations, and medication), but if the system were not in use, health-care professionals would devise workarounds, ask for information from the patients themselves, or perform further tests to discover issues. These activities would create significant extra work, increase risks due to missing or incorrect information, and reduce patient safety, since medical information or medical allergies, for example, might not be known (IT department B; Health-care personnel A–H). Increased rush and operational

congestion, in particular, were seen as problematic, since workarounds would not be as efficient as regular activities. Information would need to be transferred personally or by couriers (IT department A–D, Management A–B, Health-care personnel A–H). This would increase the stress experienced by the health-care personnel and the patients. In the worst case, patient safety measures would be reduced due to delayed care or malpractice. These consequences would add up if the attack, or system downtime, were to be prolonged. With shorter breaks of up to a few hours, less urgent operations could be postponed, and only acute operations would be conducted. If the situation were to be prolonged, the queues would get longer, and less urgent cases might turn into acute ones. The problem would be even worse if accidents were to happen while the hospital was being cyberattacked. The number of critical and urgent cases would then quickly exceed the care capacity (Health-care personnel B, H).

We also identified data leakage and identity theft. Patient records can be stolen, or they can accidentally be leaked. Such data might be used for blackmailing or threatening innocent patients (IT department A, Health-care personnel E). Although patient data leakages target individual patients and their privacy, the hospital is responsible for its patients and for securing their information. Data theft might thus result in regulatory sanctions and loss of reputation (IT department A–D, Management A, B, Health-care personnel A, B, D). The managers emphasized the loss of reputation and were afraid that their services would no longer be trusted. In addition to data theft, reputation could be lost due to mistakes, malpractice, or it becoming impossible to provide care. If patients envisioned that they or their personal and medical information were not secure, the hospital would have to react to those fears (IT department A–D, Management A–B, Health-care professionals A, B, D).

"*Maybe the most severe and difficult situation would be the modification of patient records without anyone noticing and operations continuing as usual*" (IT department B). In particular, modifying critical data, such as blood type or medical allergies, would have fatal consequences (Health-care personnel B, D, E, H). It would be challenging to identify these changes if the system otherwise operated correctly (IT department B).

In addition to the immediate effects, a cyberattack could also have other consequences. These would include the larger costs and budgetary problems caused by additional personnel, recovery activities from workarounds such as manually typing handwritten notes into the patient record system, replacing or fixing broken systems and equipment, and sanctions for data regulation violations. The financial consequences that might emerge would be handled later, and these could have an impact on the hospital long after the acute cyberattack had been resolved (IT department A–B, Health-care personnel A, D).

4.2 Preparing for Cyberattacks and Building Resilience

The interviewees pointed out that preparation for cyberattacks was maintained through the following five initiatives: (1) raising general awareness of cyberattacks through lectures and training materials, (2) management training and improving their communication and decision-making processes, (3) creating recovery instructions for different cyberattack situations and ensuring the availability of those instructions, (4) protecting existing IS, and (5) measuring the readiness of the other four activities.

The activities to **raise awareness** of cyberattacks and their impact were mostly in the form of lectures and educational materials, such as how to detect when a computer is under attack and how such attacks should be reported. Participating in the lectures or studying the materials was not compulsory, so it was mainly those who already had an interest in the topic who invested their time in this action. This leads to the problem of many individuals being unaware of or not motivated to study cyberattacks and how they can impact their work.

The need for **cyberattack-related training** was identified by the hospital's top management, who regularly practiced responses to different crises. Cyberattack-related training involved the executive team, IT department, external IT partner, and health-care managers. The interviewees who had participated in them considered them to be beneficial. The training increased not only the decision-makers' readiness to act efficiently and collaborate with others but also to evaluate the existing instructions. As one of the IT managers noted: "*Instructions need to be designed carefully and*

distributed throughout the organization. But how they work when [the cyberattack] hits us, we don't know. For this reason, training is important for everyone" (IT department, B).

While there had been significant efforts to provide management-level training, cyberattack training was not offered to blue-collar care workers. The reason for this was that care workers should continue as usual, no matter what was happening. Despite the absence of training, the health-care personnel felt that other challenging situations had improved their preparedness for cyberattacks. For instance, the COVID-19 pandemic had emphasized their ability to adapt to fast-changing instructions and process changes, and regular IS updates forced into practice paper-based care provision. However, system shutdowns would typically be known beforehand, so that critical information could, for instance, be printed out in advance.

Creating recovery instructions and ensuring their availability was one of the main practices used to increase preparedness for cyberattacks. Similar to training sessions, the instructions mostly targeted the IT department, top managers, and an ad hoc coordination team established to resolve attacks. These instructions emphasized outside communication and the right to make public statements. For the care units, the instructions proposed and assumed that care should be provided as normally as possible. There would be many situations (e.g., surgery and labor) that would continue even if an attack were detected. The health-care personnel thus needed to focus on their core task, which was health care, not on the resolution of the attack.

Some departments had developed printed cards that defined what their health-care personnel were supposed to do. However, most health-care personnel do not know where to find such instructions or what they should do when access to the intranet was prevented. A health-care coordinator recognized this risk: *"Alternative operations should be internalized. One should not rely on IS. Every unit should have a plan for what to do when something happens. I am very proud that in [our unit], we are prepared. Every process has been thought through from the beginning. Others might not have as good a situation*" (Health-care personnel, E).

Protecting organizational information systems was considered critical for securing and preparing the hospital against cyberattacks. The most critical IT infrastructure had been duplicated. Thus, if medical devices or systems were to be attacked or damaged, they could be disconnected or isolated from the remaining IS infrastructure and then replaced. While the duplication was considered to have improved the organization's ability to recover from cyberattacks, it also improved fault tolerance and increased the flexibility of the infrastructure.

These four initiatives steered how the hospital **measured its preparedness** for cyberattacks. However, many interviewees pointed out they did not have a good overview of whether they themselves were sufficiently prepared for a cyberattack and wanted their capabilities to be assessed. The initiatives improved the hospital's ability to react to cyberattacks and build its resilience.

4.3 Problems Hindering Resilience

The hospital had invested significantly in preventing and recovering from cyberattacks. However, there were also several issues hindering the process of building the ability to react to cyberattacks and improve resilience capabilities. For example, despite the efforts to raise awareness, the hospital continued to suffer from attitude problems and ignorance towards cyberattacks. This was especially the case with communication problems between the departments and management and instructions not reaching all parts of the hospital. The IT department and the IT partner had done their share of protecting the IS, but many medical devices had poor security. The device manufacturers were not interested in security improvements. Lastly, there was insufficient understanding of how to identify, respond to, and recover from cyberattacks successfully.

While the hospital had aspired to improve awareness of cyberattacks through lectures and training materials, the interviewees agreed that it suffered from **attitude problems**, especially concerning the willingness to contribute to preventing attacks. To protect the IS, the IT department required committed

personnel to perform system updates and to detect cyberattacks that had passed its defense mechanisms. The IT department and management were frustrated that the health-care personnel were indifferent regarding cyberattack prevention. "*When, for instance, security updates are performed, every option is bad. [Our health-care personnel] think: 'Can't you understand that I am busy, and there is no good time [for the update]?' They should understand why we are carrying out [these updates]. Updates are made because there are so many bad guys who are improving their tactics. […] This is a constant race. We try to make this easy for the personnel, but every once in a while, they just have to let the computer update*" (IT department D).

The IT department felt that the health-care personnel did not consider the threat of cyberattacks seriously enough. This was seen to be caused by poor awareness of cyberattacks and their threats and risks. This is surprising, since "*the [recent, tabloid-reported attack on a private mental health organization] also woke us up to think about these things, but what kind of problems would we need to have so that we would be able to consider [IT security] on time? I really hope that it will not be necessary, but we seem to always learn the hard way*" (Health-care personnel, C).

The interviewees were unanimous that a cyberattack would do significant harm to patients. However, while the potential harm was acknowledged, there remained low enthusiasm among the health-care personnel for contributing to cyberattack prevention. They did not understand the versatility of different cyberattacks or believe that a cyberattack could happen in their organization. "*It is very difficult to imagine that someone would actually do something like that, but still, [attacks] happen. What kind of impact can [cyberattacks] have, and how much and in which ways we can prepare? These are the things we need training for*" (Health-care personnel, F).

They also said that cyberattacks were the responsibility of the IT department: *"Couldn't the IT people come up with something so that we would not have to be afraid all the time, whether at work or at home?*" (Management, B).

Communication problems were extensively discussed. While the external communication protocol, such as from the hospital to the press, was well defined, internal communication was not. There were explicitly defined communication routes for system downtimes, but the social perspective was somewhat missing. For instance, it was stated that certain managers were responsible for communicating with their subordinates, but it was not clear who was to take the lead if they were not available during an attack. "*We should start thinking about communication and its impacts right away. In this type of situation, there are fast emerging impacts that affect patient care. It is the first thing that needs to be considered in outside communication but also internally, to the employees*" (Management, A).

In addition to the challenge of information flow, there were problems in creating a shared language. The management-level interviewees were frustrated that the IT department lacked contextual understanding and that its staff were not able to communicate with the management in language that they could understand, relying instead on technical jargon. This problem was also apparent among IT staff: "*Our IT partner suggested that we should isolate one machine and take it out of use. Thit means that the machine is then no longer available for care provision and will impact the patients' safety. The management team will make the decision if the precaution is to be taken.* […] *We should be better at presenting things to the management. They are not interested if some server is down; that tells them nothing. We should ourselves understand the impact that a server that is down will have on care. The managers can then make a decision on whether [the situation is] serious or not*" (IT department, A).

A similar kind of disparity in preparedness was present between the units, and there were **significant differences in internal instructions**. For example, one health-care personnel member said: *"To get ready for this interview, I went and checked it out. As far as I know, our unit has no guidelines, and I could not find any instructions regarding cyberattacks on our intranet either. […] If we were to face [a cyberattack] and quickly looked for instructions on our intranet, we would not find them*" (Health-care personnel, F). The lack of instructions reflected the lack of appreciation for cybersecurity issues. The health-care personnel felt that much had been invested in generic security issues but cybersecurity had

been ignored: "*We put lot effort on fire and personnel safety in the monthly security surveys, but information and system security are in their infancy, in our unit, at least*" (Health-care personnel, F).

Medical devices had their own issues. While the IT department had great interest in improving the security of systems and devices, its hands were usually tied. Many device manufacturers were specialized and had a significant market share, so they had no real competitors. The hospital had to acquire the devices it needed, regardless of their security level. For manufacturers, device security was not considered a key priority or a market-winning strategy. Despite the shared efforts of several hospitals, improvements were slow. Many medical devices undermined cybersecurity.

Although the interviewees criticized the hospital's preparedness for cyberattacks and its general level of resilience, they felt that there was a good safety culture. However, since the hospital was large, its size created significant challenges in providing a good **overview of the organizational situation on the readiness for cyberattacks**. Consequently, a shared understanding of the organization's status and ability to identify, respond to, and recover from cyberattacks remained unknown. For example, there was no clear view of how the health-care personnel should act when the hospital was under attack. The employees acknowledged that the operations should proceed as normally as possible; however, there was some uncertainty and lack of clarity about how they should actually address this. The health-care personnel had concerns about the IT department and the external IT partner's insufficient understanding of the hospital context and the extent to which their suggestions might impact care provision. Instead, the hospital focused on preventing attacks, not activities during or after an attack. In other words, its level of resilience was relatively low.

5 Discussion

Our case study shows how an organization has built its capability to react to unexpected situations; that is, how it has tried to improve its resilience at the organizational level. As the hospital example illustrates, preparing for cyberattacks is not an easy task in large organizations. In the case at hand, cyberattack preparation measures seemed to focus on improving robustness against different attack scenarios. While some activities and challenges were technical, such as protecting existing IT and IS and challenges with unsecured medical devices, most issues were non-technical by nature.

Here, we focus especially on the non-technical activities, most of which aim to help the organization and its employees continue the provision of care no matter what happens. In this respect, the hospital's preparation activities worked reasonably well. The activities to raise awareness, at least based on the threats and potential consequences identified by the interviewees, had been successful—to some degree—and the means of training, instruction, and technical prevention had been developed and distributed to the appropriate receivers. On the other hand, the challenges that related to the hospital employees' attitudes created a significant problem. While the staff had identified and partly acknowledged the risks of cyberattacks, they did not see themselves as actors in terms of improving cybersecurity or general resilience. The principle that the care personnel would continue to provide care even during a cyberattack or other crises distanced them from any resilience improvement. The preparedness for cyberattacks seemed to be related only to IT people and top management.

The cyberattack training was targeted at the management and IT staff, which improved the hospital's ability to operate under attack. For instance, identifying the challenges, such as with communication, during the training sessions enabled the hospital to proactively improve its processes. Since proactiveness is a core feature of resilient organizations (Braunscheidel and Suresh, 2009; Shukla et al., 2011), training, even when offered to a limited target group, is an important activity for improving cyberattack resilience.

The training also enabled feedback to be provided on different instructions. Such instructions are critical during and after crises because they increase the robustness of the hospital and improve its resilience. However, as the interviews showed, these instructions were not consistent, coherent, or made available throughout the organization. Similar kinds of deficiency were also apparent in measuring organizational

readiness. They seemed not to have a good overview of the hospital's capability to prevent, survive, and recover from cyberattacks or its resilience.

Nevertheless, we believe this situation and these shortcomings are not unique. The activities the hospital had undertaken to prepare for cyberattacks are in line with earlier suggestions (Hubbard et al., 2017). Also, these challenges are not new (Bada et al., 2015). When the activities and challenges were observed from an organizational resilience point of view (Burnard and Bhamra, 2011), it seems that most of them focused on operational robustness; that is, regardless of the situation, care providers should not be disrupted. This approach might be adequate for short-term problems but easily becomes an issue if, for example, essential IS and patient records were not available or usable for a prolonged period of time.

Improving both cybersecurity and organizational resilience requires a collaborative effort from all actors in an organization (Rajivan and Cooke, 2017). Instead of individuals working alone to survive and learn from crisis situations, groups and individuals need to work together to mitigate the possible consequences of different crises (Goldstein, 2012). In this sense, while activities to increase awareness had prepared the hospital to identify the threats, this had not necessarily improved its ability to cope with an attack when it occurred or recover after it.

These notions were collected into a framework for analyzing and improving organizational resilience (see Figure 1). First, we divided the process of improving resilience into three main phases: before, during, and after a possible crisis (e.g., a cyberattack). We borrowed these temporal phases from previous research in the context of resilience (Maruyama et al., 2014; Weber et al., 2021) and from studies of disaster management (Lettieri et al., 2009) and business continuity management (Jain et al., 2020; Niemimaa et al., 2019). They are useful for studying and structuring behavioral activities over time. Next, referring to our findings, we stated that health-care organization needs a certain set of prerequisites, such as competences, skills, and organizational processes, to prepare for possible threats and upcoming crises (Gallopín, 2006; Kurtz and Varvakis, 2016; Välikangas and Romme, 2012). Based on our data collection, these measures included preparatory measures, such as education and training, to increase awareness of cyberattacks among departments. However, the respondents criticized, for example, attitude problems and, as a result of them, there was a low level of commitment on the part of individuals to update their information systems.

Our framework (see Figure 1) synthesizes the results and provides a basis for further research to advance the concept of organizational resilience. We also see the potential to explore the framework in other contexts and believe that researchers will come up with similar results. Finally, we believe that health-care organizations, which are often referred to in the literature as high-reliability organizations (e.g., Desai et al., 2016), are in general much more aware of potential risks. Accordingly, we assume that they prepare themselves much more consciously and intensively for different risks. In addition, we see a potential to compare our case with other hospitals in Finland or within Europe. During the discussions with the practitioners of the field, we discovered that different hospitals have different ways of operating. Thus, it would be interesting to study whether these differences lead to different results.

We make use of three temporal phases (prevention, reaction, recovery) to structure the current activities and responsibilities initiated by the hospital to prevent cyberattacks and thus improve its organizational resilience. For example, in the case of cyberattacks, the whole organization monitors unexpected incidents in the IS and among the health-care personnel as a part of their care activities and the IT staff as their (or someone's) main job. During an attack, the IT staff focus on stopping it while the health-care personnel care for patients in the best possible way. During the recovery phase, the groups work together to find ways to return to a normal situation. Similarly, the management tasks vary from phase to phase.

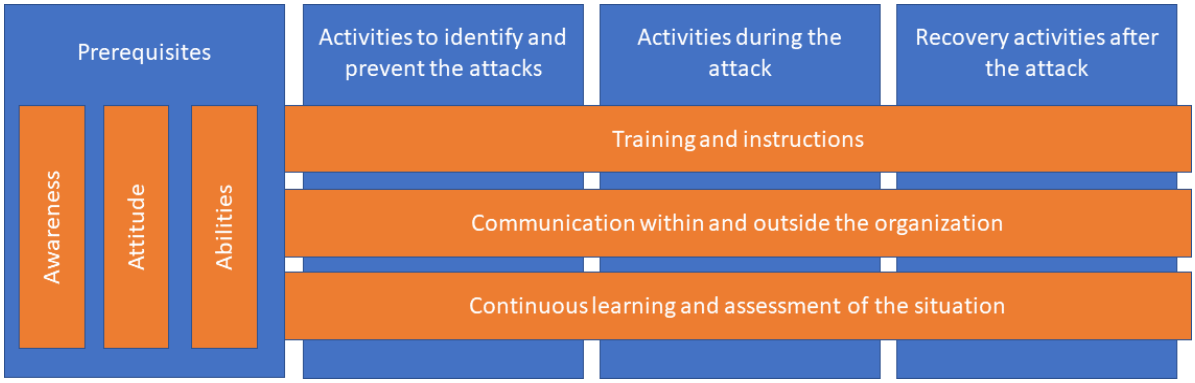

Figure 1. Framework for analyzing and improving organizational resilience.

Training and instructions should be targeted to the whole organization and provide adequate information to each actor that is aptly tailored to their tasks in each phase. As each actor receives the appropriate information, the internalization of the instructions is also improved. The training sessions provide feedback for assessment learning and further improve organizational resilience. Communication should be active both inside and outside the organization. These findings reflect earlier studies which point out that organizations need to learn to deal with turbulent changes and disruptions. In particular, they must learn which vulnerabilities can lead to such adverse events (e.g., Fiksel et al., 2015).

A retrospective analysis of our case hospital using our framework showed that its focus was very fragmented. It did the right things by providing training and developing instructions, but since there were severe problems with the prerequisites (awareness of cyberattacks, the attitudes of the personnel, and the ability to distribute instructions and deliver training), the instructions and guidelines were not effectively internalized. An instruction remained a distant piece of advice and did not meet the organizational reality of the health-care units.

6 Conclusion

In this paper, we applied a single qualitative case study to identify how to prepare for cyberattacks at the organizational level. Our case offers insights into how an organization prepares for cyberattacks and consequently improves its organizational resilience. To synthesize the results, we developed a framework and have provided some lessons learned, supporting practitioners and researchers to study resilience at the organizational level. It should be emphasized that the hospital saw cyberattacks mainly as being related to IT staff and top management. In contrast, we identified a lack of sufficient education and awareness training for health-care personnel to respond appropriately. From a practical perspective, this can be vital in the event of a prolonged IT shutdown.

Finally, our study does not come without limitations. Our single case study is limited to the health-care context, and thus generalizing the details to other contexts should be done cautiously. However, we found a considerable amount of previous work dealing with similar topics, such as increasing awareness or realizing preparatory measures. Furthermore, our results should be interpreted cautiously if they are applied to smaller or privately financed hospitals. Without substantiating this fact, we believe that large government-funded hospitals (as our case organization) may be differently capitalized and managed, leading to different types of training or even larger investment in preparing for cyberattacks.

References

Bada, M., Sasse, A.M., Nurse, J.R., 2015. Cyber security awareness campaigns: Why do they fail to change behaviour? Presented at the International Conference on Cyber Security for Sustainable Society, pp. 118–131.

Berg, S.H., Akerjordet, K., Ekstedt, M., Aase, K., 2018. Methodological strategies in resilient health care studies: an integrative review. Safety Science 110, 300–312.

Bhamra, R., Dani, S., Burnard, K., 2011a. Resilience: the concept, a literature review and future directions. International journal of production research 49, 5375–5393.

Bhamra, R., Dani, S., Burnard, K., 2011b. Resilience: The Concept, a Literature Review and Future Directions. International Journal of Production Research 49, 5375–5393.

Bhosale, K.S., Nenova, M., Iliev, G., 2021. A study of cyber attacks: In the healthcare sector. Presented at the 6th Junior Conference on Lighting, IEEE, pp. 1–6.

Boddy, A., Hurst, W., Mackay, M., Rhalibi, A.E., 2017. A study into data analysis and visualisation to increase the cyber-resilience of healthcare infrastructures, in: Proceedings of the 1st International Conference on Internet of Things and Machine Learning. pp. 1–7.

Boudko, S., Abie, H., 2019. Adaptive cybersecurity framework for healthcare internet of things. Presented at the 13th International Symposium on Medical Information and Communication Technology (ISMICT), IEEE, pp. 1–6.

Braunscheidel, M.J., Suresh, N.C., 2009. The organizational antecedents of a firm's supply chain agility for risk mitigation and response. Journal of Operations Management 27, 119–140.

Burnard, K., Bhamra, R., 2011. Organisational resilience: development of a conceptual framework for organisational responses. International Journal of Production Research 49, 5581–5599.

Coventry, L., Branley, D., 2018. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas 113, 48–52.

Desai, V., Madsen, P.M., Roberts, K.H., 2016. High-reliability organizations in health care, in: Handbook of Human Factors and Ergonomics in Health Care and Patient Safety. CRC Press, pp. 202–213.

Eisenhardt, K.M., 1989. Building Theories from Case Study Research. The Academy of Management Review 14, 532–550.

Fiksel, J., Polyviou, M., Croxton, K., Pettit, T., 2015. From Risk to Resilience: Learning to Deal With Disruption. MIT SMR 56, 19–34.

Gallopín, G.C., 2006. Linkages between vulnerability, resilience, and adaptive capacity. Global environmental change 16, 293–303.

Goldstein, I., 2012. Empirical Literature on Financial Crises: Fundamentals vs. Panic, in: Caprio, G., Beck, T., Schmukler, S.L. (Eds.), The Evidence and Impact of Financial Globalization. Citeseer, pp. 523–534.

Hillmann, J., 2021. Disciplines of organizational resilience: contributions, critiques, and future research avenues. Review of Managerial Science 15, 879–936.

Hillmann, J., Guenther, E., 2021. Organizational resilience: a valuable construct for management research? International Journal of Management Reviews 23, 7–44.

Hubbard, T., Weber, T.G., Steinhoff, J.C., 2017. Protecting data assets in a perilous cyber world. The Journal of Government Financial Management 66, 26–31.

Jain, P., Pasman, H.J., Mannan, M.S., 2020. Process system resilience: from risk management to business continuity and sustainability. International Journal of Business Continuity and Risk Management 10, 47–66.

Jeffcott, S.A., Ibrahim, J.E., Cameron, P.A., 2009. Resilience in healthcare and clinical handover. Quality and Safety in Health Care 18, 256–260.

Kelli, V., Sarigiannidis, P., Argyriou, V., Lagkas, T., Vitsas, V., 2021. A cyber resilience framework for NG-IoT healthcare using machine learning and blockchain. Presented at the IEEE International Conference on Communications, IEEE, pp. 1–6.

Kohn, V., 2020. How the Coronavirus Pandemic Affects the Digital Resilience of Employees, in: Proceedings of the 41st International Conference on Information Systems. Hyderabad, India, pp. 1–17.

Kurtz, D.J., Varvakis, G., 2016. Dynamic capabilities and organizational resilience in turbulent environments, in: North, K., Varvakis, G. (Eds.), Competitive Strategies for Small and Medium Enterprises: Increasing Crisis Resilience, Agility and Innovation in Turbulent Times. Springer, Cham, Switzerland, pp. 19–37.

Lettieri, E., Masella, C., Radaelli, G., 2009. Disaster management: findings from a systematic review. Disaster Prev and Management 18, 117–136.

Linnenluecke, M.K., 2017. Resilience in Business and Management Research: A Review of Influential Publications and a Research Agenda: Resilience in Business and Management Research. International Journal of Management Reviews 19, 4–30.

Maruyama, H., Legaspi, R., Minami, K., Yamagata, Y., 2014. General resilience: taxonomy and strategies. Presented at the International Conference and Utility Exhibition on Green Energy for Sustainable Development (ICUE 2014), IEEE, pp. 1–8.

Murray, M., 2018. Qualitative interviews, in: Flick, U. (Ed.), The SAGE Handbook of Qualitative Data Collection. Sage Thousand Oaks, CA, pp. 264–279.

Niemimaa, M., Järveläinen, J., Heikkilä, M., Heikkilä, J., 2019. Business continuity of business models: Evaluating the resilience of business models for contingencies. International Journal of Information Management 49, 208–216.

Nifakos, S., Chandramouli, K., Nikolaou, C.K., Papachristou, P., Koch, S., Panaousis, E., Bonacina, S., 2021. Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors 21, 5119.

Pedersen, K.Z., 2016. Standardisation or resilience? The paradox of stability and change in patient safety. Sociol Health Illn 38, 1180–1193.

Pekkola, S., Hekkala, R., Rossi, M., Smolander, K., 2019. The magical "we": Enhancing collaboration transparency in grounded theory method in information systems research. Communications of the Association for Information Systems 45, 16.

Rajamäki, J., Pirinen, R., 2017. Towards the cyber security paradigm of ehealth: Resilience and design aspects. Presented at the Proceedings of the AIP Conference, AIP Publishing LLC, pp. 1–9.

Rajivan, P., Cooke, N., 2017. Impact of team collaboration on cybersecurity situational awareness, in: Liu, P., Jajodia, S., Wang, C. (Eds.), Theory and Models for Cyber Situation Awareness. Springer, Cham, Switzerland, pp. 203–226.

Rangachari, P., Woods, J.L., 2020. Preserving organizational resilience, patient safety, and staff retention during COVID-19 requires a holistic consideration of the psychological safety of healthcare workers. International Journal of Environmental Research and Public Health 17, 4267.

Roulston, K., Choi, M., 2018. Qualitative interviews, in: Flick, U. (Ed.), The SAGE Handbook of Qualitative Data Collection. Sage Thousand Oaks, CA, pp. 233–249.

Safavi, S., Meer, A.M., Melanie, E.K.J., Shukur, Z., 2018. Cyber vulnerabilities on smart healthcare, review and solutions. Presented at the Cyber Resilience Conference (CRC), IEEE, pp. 1–5.

Sarkar, A., Wingreen, S.C., Cragg, P., 2017. CEO Decision Making under Crisis: An Agency Theory Perspective. Pacific Asia Journal of the Association for Information Systems 9, 1–22.

Sethuraman, S.C., Vijayakumar, V., Walczak, S., 2020. Cyber attacks on healthcare devices using unmanned aerial vehicles. Journal of Medical Systems 44.

Shukla, A., Agarwal Lalit, V., Venkatasubramanian, V., 2011. Optimizing efficiency-robustness trade-offs in supply chain design under uncertainty due to disruptions. International Journal of Physical Distribution & Logistics Management 41, 623–647.

Siponen, M.T., Oinas-Kukkonen, H., 2007. A review of information security issues and respective research contributions. ACM SIGMIS Database: the DATABASE for Advances in Information Systems 38, 60–80.

Sood, A., Moidu, K., 2018. Protection of healthcare information: Adding cyber resilience and recovery. Presented at the International Conference on Computational Science and Computational Intelligence (CSCI), IEEE, pp. 132–134.

Thomas, G., 2011. A typology for the case study in social science following a review of definition, discourse, and structure. Qualitative Inquiry 17, 511–521.

Välikangas, L., Romme, A.G.L., 2012. Building resilience capabilities at "Big Brown Box, Inc." Strategy & Leadership 40, 43–45.

Walsham, G., 2006. Doing interpretive research. European Journal of Information Systems 15, 320–330.

Walsham, G., 1995. Interpretive case studies in IS research: nature and method. European Journal of information systems 4, 74–81.

Wang, C.-H., Liu, G.H., Lee, N.C.-A., Chen, K.-J., 2019. Passive leadership and online interaction: the mediating effects of job autonomy and employee resilience, in: Proceedings of the 23rd Pacific Asia Conference on Information Systems (PACIS 2019). pp. 1–15.
Weber, M., Hacker, J., vom Brocke, J., 2021. Resilience in Information Systems Research - A Literature Review from a Socio-Technical and Temporal Perspective, in: Proceedings of the 42nd International Conference on Information Systems (ICIS 2021). Austin, Texas.
Wieland, A., Wallenburg, C.M., 2013. The influence of relational competencies on supply chain resilience: a relational view. International Journal of Physical Distribution & Logistics Management 43, 300–320.
Zhang, J., Li, L., Lin, G., Fang, D., Tai, Y., Huang, J., 2020. Cyber resilience in healthcare digital twin on lung cancer. IEEE Access 8, 201900–201913.
Zhang, J., Tai, Y., 2022. Secure medical digital twin via human-centric interaction and cyber vulnerability resilience. Connection Science 34, 895–910.

Appendix: Interview Questions

Personal Introduction
Could you introduce yourself and provide a description of your responsibilities in the hospital.

Cyberattacks - General
How are cyberattacks detected in the organization? / How would you get the information of an ongoing cyberattack?
When a cyberattack is detected, what happens? Why?

Governance
In your opinion, does everyone knows what they are supposed to do during an attack? Do they have the necessary information? How do they see their tasks?
Who will do what and why?

Potentials and Challenges
What are the potential consequences of a cyberattack?
What potential challenges could you face during a crisis situation? What problems could arise?

Measures and Procedures
Do you measure your preparedness for cyberattacks in some way?
How do the operations return to normal after an attack?

Concluding Questions
Who do you think we should interview next?