Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P017-cd

On the cyber-emergency preparedness in a resilient organization

Anurag Shukla

Information technology, Institute for Energy Technology, Norway. E-mail: Anurag.Shukla@ife.no

Even Andre Solbakken

Emergency and HSE Nuclear Sector, Institute for Energy Technology, Norway. E-mail: Even.Solbakken@ife.no

Riana Steen

Accounting and Operations Management, BI Norwegian Business School, Norway. E-mail: Riana.Steen@bi.no

In recent years, the scientific fields of cyber-security and resilience engineering have emerged as new ways to deal with emerging risks in cyber-socio-technical systems. Unlike conventional security management approaches, focusing on historical data to provide an accurate risk picture, resilience engineering aims to enhance an organization's capacity to anticipate, monitor, and adapt to disruptions and surprises. However, with the increasing cyber threats and changes in national and international security policies, there is a pressing need to examine the resilience characteristics of cyber emergency preparedness in both the public and private sectors. To address this need, this study adopts a triangulation method through an online survey and interview with two subject matter experts in the cyber domain. It explores factors that might contribute to enhancing cyber emergency preparedness in dealing with potential cyber threats and attacks. Findings suggest that front-line operators have limited information and capacity to process existing data in the domain of cyber security, highlighting a need for enhancing cyber-related knowledge across organizations. Furthermore, 25% of enterprises in the sample update their cybersecurity risk picture only once a year. The lack of more frequent updates downscales the contingency plans' thoroughness and puts companies in a vulnerable situation, given the increasing trend of cyber-attacks.

Keywords: Risk, Risk Management, Risk Assessment Resilience Engineering, RAG, Cyber-Socio-Technical Systems, Security Culture, Emergency Response Preparedness, Cyber Incident, Cyber Security

1. Introduction

The contemporary business environment is abounding with uncertainty. The forces of globalization, digitalization, and evolving national and international cyber threats (ENISA, 2022) have resulted in an increased frequency of cyber-attacks targeting critical infrastructure, presenting new challenges for organizations (Henrie, 2013). To attain strategic objectives in such intricate environments, it is imperative to enhance an organization's adaptive capacity to confront these challenges (Tangenes & Steen, 2017). Risk management (RM) is a central aspect of this endeavor. The idea of RM, according to Prior and Hagmann (2014), is both prevalent, as it is regarded as an essential component of decentralized, proactive measures for tackling complex threats, as it is viewed as a crucial element of decentralized, anticipatory measures for addressing complex threats regardless of their type, and enigmatic since its practical implementation is as varied as its definitions. A main element in security RM is cyber-preparedness activities, aiming to ensure that organizations have the necessary measures in place to detect, prevent, respond to, and recover from cyber incidents (ENISA, 2022). Such preparedness activities may include conducting regular cybersecurity risk assessments (RA), implementing security controls and procedures, providing cybersecurity training to employees, and developing incident response plans. An imbalance in cyber-preparedness and desired outcomes can create significant challenges in dealing with cyber-attacks when they occur. Insufficient preparedness to handle cyber-attacks can lead to significant damage by reducing an organization's functionality and operational continuity (Phillips & Tanner, 2019). Several scholars (Aven & Thekdi, 2018; Ferdinand, 2015; Petruzzi & Loyear, 2016) propose that enhancing the RM process necessitates adopting comprehensive methods. In this study, the term "holistic" is employed to contrast with an asset-centered approach, which fails to adequately consider the crucial interrelationships and close linkages among various components of the system. To this end, the paper builds on the premise that resilience engineering (RE) concepts and tools provide the necessary grounds for adopting a holistic RM approach in a cyber-security context. Resilience is characterized by four main characteristics: anticipating future developments and threats, monitoring emerging risks, responding effectively to regular and irregular disturbances, and proactively learning from experience (Hollnagel, 2013).

To comprehensively investigate these characteristics, it is essential to have a deep understanding of the context in which cyber-preparedness activities are carried out. This paper aims to investigate the factors that contribute to improving resilience in cyber emergency preparedness among enterprises, using resilience engineering (RE) concepts and their application in the field of security management. To achieve this goal, this exploratory study employs a triangulation method in three phases. The first phase involves a review of relevant literature to develop a questionnaire and interview guide. In the second phase, data is collected through web-based surveys with 28 key informants and two semi-structured interviews with subject matter experts in the cyber-domain, utilizing both qualitative and quantitative data. In the third phase, we analyze the data collected in the second phase and identify several areas of improvement that could have an impact on cyber-preparedness in organizations.

The paper concludes that strengthening cyber-preparedness and cyber-security is crucial for organizations due to the increased risk of cyber threats and cross-border crime. Basic principles for IT security also play an essential

role in contributing to a greater degree of resilience in businesses.

2. Two security risk management approaches: systematic and systemic

The main aim of conducting security RM is to improve cybersecurity RM by providing insights into the risk phenomena, processes, activities, and systems being analyzed (Alahmari & Duncan, 2020). By identifying cyber-related hazards and threats, studying their causes and consequences, and describing risk, decision-makers are informed about the risk level and the key contributors to risk (Aven, 2015). The RA supports decisions on risk acceptability (tolerability) and the selection of alternatives. RM is an integral part of good management practice. It is an iterative process consisting of steps that, when undertaken in sequence, enable continuous improvement in performance and decision-making (Aven & Renn, 2010, p. 183). What follows briefly outlines two main security RM approaches, namely systematic and systemic, concerning the adapted risk perspectives and RM approach.

2.1 *Systematic cyber-security risk management*

Systematic cyber RM, such as ISO/ICE 27005:2018 (ISO/IEC, 2018) and OCTAVE framework (Caralli et al., 2007), is based on the so-called three-factors risk perspective, combining factors of value (asset), threat, and vulnerability. It consists of the following processes: risk identification (which involves identifying assets, threats, existing controls, vulnerabilities, and potential consequences), risk analysis (including assessing the consequences, the likelihood of incidence, and determining the level of risk), and risk evaluation. RA supports finding appropriate risk treatment options and producing a risk mitigation plan (fig. 1).

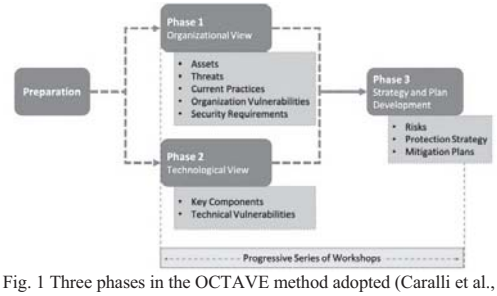

Fig. 1 Three phases in the OCTAVE method adopted (Caralli et al., 2007)

In the NIST Cyber Security Framework (Force, 2018, p. 66), the term risk is defined as "*a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.*" Three main components of risk in this definition, as for OCTAVE framework and ISO/ICE 27005:2018 are then, threat, asset, and vulnerability. The likelihood of occurrence combined with the adverse impacts indicates the level of vulnerability.

Fig. 2 shows the process of RM and how information and communication flow between components. Black arrows represent the main flows within the process, with risk framing guiding the steps from RA to risk response to risk monitoring.

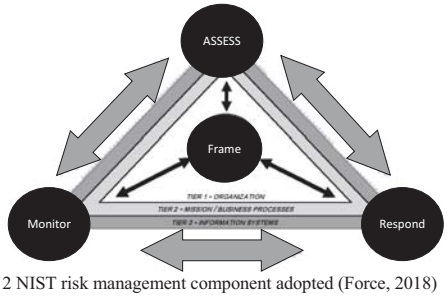

Fig. 2 NIST risk management component adopted (Force, 2018)

The risk framing component describes how organizations acquire and share threat information with the RA component. Subsequently, the RA component determines the level of risk and communicates it, along with the RM strategy, from the risk framing component to the risk response component. These inputs aid decision-makers in selecting an appropriate course of action for risk responses. For a more detailed understanding of the main activities involved in conducting RM, consider the following steps when addressing RM within enterprise architecture:

(i) Developing a segment architecture linked to organizational goals, missions, and processes.
(ii) Identifying critical risk response areas for missions and functions.
(iii) Defining appropriate security requirements based on RM strategy.
(iv) Incorporating information security architecture to implement requirements.
(v) Translating requirements into specific security controls for systems/environments.
(vi) Allocating security controls to systems and environments.
(vii) Documenting RM decisions at all levels of the architecture.

Stages five (v) and six (vi) aim to provide a safeguard likelihood- and consequence-reducing barriers. These barriers are often also used as preventive measures. After an incident has occurred, these measures are subject to evaluation in which the results use for developing and implementing "new" impact-reducing measures or barriers (Lunde, 2019, pp. 41-42).

2.2 *Systemic security risk management*

The previous section on systematic RM primarily focused on identifying inherent risks in a given system. This approach assumes that a comprehensive understanding of the system as a whole can be achieved by breaking it down into individual components and analyzing their behavior (Hollnagel, 2013). However, due to the high level of uncertainty and difficulties in anticipating security threats, an alternative approach that takes a systemic view might be more suitable, such as resilience-based RM (Aven & Thekdi, 2018; Steen, 2019).

Resilience has been defined and used in various ways and in several scientific and practical fields in recent decades. At its core, resilience refers to an organization, system, or critical infrastructure capacity to recover from disruptions, often referred to as 1) a process (Stainton et al., 2019; Cantelmi, Di Gravio, & Patriarca, 2021), 2) an ability (Holling, 1973, p. 14), or 3) a capacity (Boin & Lodge, 2016).

Resilience is also referred to as a concept that can be illustrated as an "umbrella term" and which is explained as a

mechanism that does something and is an ability and capacity that helps systems or organizations that have been exposed to disruption bounce back to square one (Nemeth & Hollnagel, 2021, p. 3; Steen, Ingvaldsen & Ferreira, 2021, p. 1), see fig. 3.

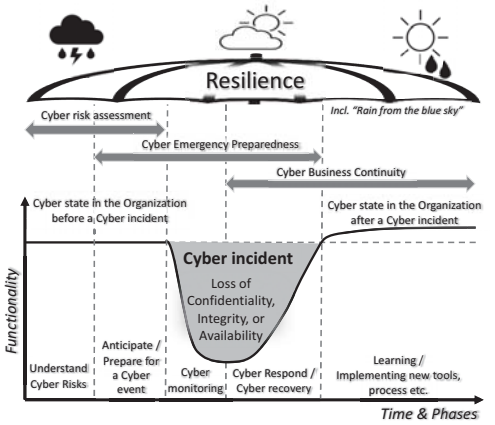

Fig. 3 The resilience in Cyber context with umbrella adopted (Øien et al., 2017)

In a security management context, the resilience umbrella illustrates that resilience includes RA, contingency planning, and restoration of functionality. A systemic approach to security RM seeks to enhance the resilience of organizations by enabling them to recognize, adapt to, and absorb disturbances. It is about moving forward from being protective to being productive in terms of security performance (Hollnagel, 2018, p. 15). By adopting a systemic perspective, organizations can increase their flexibility and adaptability to new and unexpected situations. As technology and socio-technical systems continue to evolve, the need for new approaches to cyber security management and RA becomes increasingly apparent. Resilience engineering has been proposed as a solution to address this need, as it offers a different set of principles and features. To be resilient, a system or organization must meet the four potentials (Hollnagel, 2013):

(i) Anticipating: knowing what to expect, that is, how to anticipate future developments, threats, and opportunities, such as potential changes, disruptions, pressures, and their consequences. This is the ability to address the potential.
(ii) Monitoring: knowing what to look for; that is, how to monitor that which is or can become a threat in the near term. This is the ability to address the critical.
(iii) Response: knowing what to do; that is, how to respond to regular and irregular disruptions and disturbances. This is the ability to address the actual.
(iv) Learning: knowing what has happened; that is, how to learn from experience. This is the ability to address the factual.

Incorporating resilience potential (i - iv) in security RM enhances the ability of an organization to meet challenges when dealing with unexpected circumstances (Steen & Aven, 2011). Developing an in-depth understanding of anticipating potential threats, monitoring warning signals, and continuously learning from day-to-day activities can significantly enhance awareness and competence in daily operations.

3. Methodology

Our semi-qualitative research is structured around three phases. Phase 1 involved a review of relevant literature on security RM and resilience, with a focus on identifying the factors that enhance the resilience of a security management system. By reviewing existing literature, we identified key themes, concepts, and gaps in knowledge related to cyber-preparedness. Once we have gathered sufficient literature, we critically analyze the material to identify key themes and concepts that inform the development of our questionnaire and interview guide.

In the second phase of the study, we applied a Mixed Method Approach (MMA) (Creswell & Creswell, 2017, pp. 187-189) to collect data through surveys, document analysis, and semi-structured interviews with subject matter experts to answer the research question. Besides, comments which might point to security-related information were removed from the data. In order to create comprehensive data, we consider organizations (both public enterprises with 39% and private enterprises with 61 % in our sample).

The survey mapped the work experience and the role or function of participants. As fig. 4 illustrates, 71 % of the participants had over 20 years of work experience.

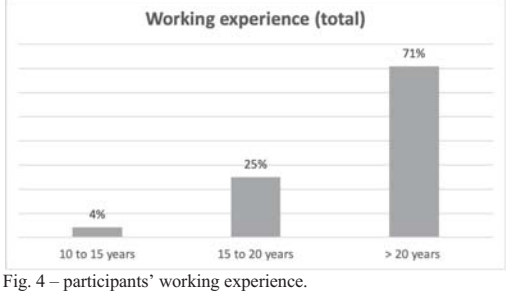

Fig. 4 – participants' working experience.

To map the size of the companies, we have used the number of employees working in the organization based on the Statistics Norway's scale (fig. 5).

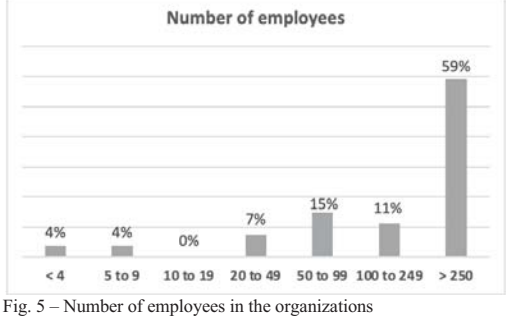

Fig. 5 – Number of employees in the organizations

After applying a purposive sampling strategy to recruit participants, we conducted two semi-structured interviews in August 2022. We selected the participants based on their knowledge about or experience with, the phenomenon of interest (Etikan, Musa & Alkassim, 2016), cybersecurity RM. The interviews lasted between 90 and 150 minutes. Each interview was recorded and transcribed into around 3500 words. After gaining consent from the subjects, we assured

them that their information would be treated in the strictest confidence and that the data would be anonymized so that no individual, incident, or organization could be identified. We looked at patterns (themes) to explain participants' comments.

In the next step, we highlighted phrases and repeated topics and assigned initial codes to articulate their content according to the study's conceptual framework, phrases and repeated topics were highlighted and assigned initial codes to articulate their content. Codes included learning, responding, monitoring, anticipating, management, risk, zero-trust, and more.

Excerpts from interviews with subject matter experts	Code grouping	Theme/Category
(1) Having an overview of systems, values, dependencies on others is important for making good plans.	**A. Learning**	**Cyber incident**
(2) They do not have an overview of how many attempts their company stops daily, weekly and monthly.	50, 52, 76, 77	J, K, L, M
(3) Have an overview of the values, I don't think most companies have a good enough overview of their values	**B. Responders**	**Resilience and Cyber Readiness**
(4) Having an overview of systems, values, dependencies on others is important for making good plans	1, 4, 5, 17, 34, 41, 52, 59, 75, 110	A, B, C, D, E, O, P, N
(5) Plans can never stand reality	**C. Monitoring**	**Risk perception**
(6) Where the CFO says you come to us and talk about this here	41, 48, 74, 75	F, G, M, P,
(7) not invited from the technical side, i.e. CISO or technological part of the business, but from the finance part	**D. Anticipate**	**Culture and emergency preparedness**
(8) What is interesting is, as I am talking about risks and what may affect them.	8, 17, 26, 41, 102	A, B, C, D, E, O, P

Fig. 6 - Excerpts from thematic analysis

After establishing the codes, in the next step, with the research questions in mind, we used the terminology from the study's theoretical background as a template to generate themes. Finally, we established 15 codes and six themes from the interview transcripts. The table (fig. 6) shows an excerpt from the template with interviews, codes, and themes.

4. Result

The results of the surveys reveal that informants and their organizations lack a common understanding of risk and do not share a consistent definition of the concept. The following results outline the findings concerning how informants and their organizations handle risk in their day-to-day operations.

- Among the participants, 54% indicated familiarity with the concept of risk. Of those familiar, 85% described risk as the product of probability and consequence.
- Regarding the maintenance of cyber risk assessments (RA), 39% reported having an up-to-date cyber-RA. Of this group, 25% updated their assessments annually, 20% updated them quarterly, and 13% updated them multiple times each month.
- The surveys revealed that the RA process in the cyber domain and the IT sectors is in an immature state. Top management showed little interest in these assessments. Cyber-risk specialists were responsible for conducting the assessments, and organizations lacked awareness of their values or did not adequately involve them in the process.

Furthermore, the surveys highlighted that the informants and their organizations also had differing understandings of resilience, lacking a shared definition of the concept. When examining the duration required to restore normal operations after a cyberattack, one of the probes yielded the following data: Findings show that the informants and their organizations have different understandings of risk and that they do not have a common description of the concept of risk. Below are some results of findings related to how informants and their organizations work with risk in practice. After analyzing the data, the findings regarding the restoration of normal operations after a cyberattack are as follows.

- The loss in production lasted for a relatively short period of three days, indicating a prompt recovery in terms of providing essential services.
- Operationally, all services were fully restored within two months after the cyberattack, demonstrating substantial recovery progress.
- Internally, it took four months to return to the normal condition, which involved activities such as restoration, and other necessary measures to ensure the organization's internal functioning.

These findings highlight the timeline and progress of recovery efforts after the cyberattack, with relatively quick restoration of essential services, followed by a longer duration for internal processes to return to their regular state. Upon analyzing the data, the following results and findings emerged regarding how informants and their organizations handle resilience in practical terms.

- There is a lack of comprehensive understanding of the IT landscape, including values and dependencies necessary for developing effective contingency plans.
- Among the respondents, 60% indicated that they were aware of or have experienced one or more cyber incidents within their organization, highlighting the prevalence of such incidents.
- It was observed that 90% of the respondents agreed that they report negative events, while 50% agreed that they do not report positive events. This indicates a potential bias towards reporting negative incidents and a potential under-reporting of positive events.
- Approximately 12% of the respondents expressed a reluctance to share information due to ongoing police investigations or statutory confidentiality, governed by the Security Act of 2018.

When these aforementioned results were presented to the experts who participated in the survey, they did not express surprise at the findings, indicating that the identified issues were already anticipated or expected based on their expertise and experience.

5. Discussion

Organizations are facing significant challenges within the Cyber domain; as we have seen in the past, these are complex (Dawson & Thomson, 2018). Most organizations have adopted digital solutions that increase efficiency, quality, and value creation. With these new digital solutions also come vulnerabilities that threat actors exploit, where the consequences can be severe for any organization, as we see this daily in the news. Some organizations are affected by different types of cyber incidents, several vulnerabilities in applications or systems, and new kinds of vulnerabilities are discovered (ref. fig. 3 "*Rain from the blue sky*").

Let's look at an example with new vulnerabilities, where threat actors try to deceive us humans by manipulating us with e-mails to click on the links or malicious attachments. Many such manipulated e-mails have been very well designed, and it can be difficult to tell them apart. Threat actors have adopted modern technology using artificial intelligence (AI) and machine learning where the message in the e-mails is made even better and more personal by putting together available information from the internet (social media), personal information from data breaches (username, password, secret

code, address, payment details, etc.). The e-mail contents are becoming good, making distinguishing e-mails with dishonest intentions harder. ENISA analyzed over 600 cyber incidents from May 2021 through June 2022, identifying at least 47 threat actors (ENISA, 2022). Most of these have financial gain as motivation, and several factors also point to state actors. In the backdrop of the war in Ukraine, in early 2023, the Ukrainian cyber security authorities discovered a new type of vulnerability in one of the most widely used e-mail solutions in organizations (Microsoft Exchange Server), where the vulnerability is being actively exploited by sending e-mails to the users and Its organization's e-mail server. Such e-mails are often referred to as phishing e-mails to trick us. In this case, the usernames and encrypted passwords in the organization's IT systems are sent back to the threat actors. Even if the password is encrypted, threat actors will be able to tabulate encrypted passwords with databases where the password is known (rainbow hashing the password). Organizations that have not adopted multiple barriers using multi-factor authentication or the Zero-trust approach, these organizations will be extra vulnerable to cyber incidents. This event's uniqueness is that the user has neither opened the e-mail nor clicked on any links or attachments. In other words, no one has been scammed or exploited with a phishing e-mail, but an unknown vulnerability in the e-mail system has been exploited and used (Works & Matters, 2023).

When threat actors manage to exploit the vulnerabilities and carry out a successful cyber-attack by, for example, extracting large amounts of data before data is encrypted and demanding a ransom from the organization. Has this way of doing business evolved further by extortion of end users? Hypponen (2021) refers to an example where a threat actor has first attacked a healthcare institution and extracted highly sensitive patient records. When they did not get the desired result from the health organization, the focus shifted to blackmailing the patients; if they did not pay the ransom, they would publish their highly sensitive patient records online (Hypponen, 2021). The situation described above highlights the critical importance of having a comprehensive understanding of risk in the context of security management. Aven (2016) suggests that "*the way we understand and describe risk strongly influences the way risk is analyzed, and hence it may have serious implications for risk management"*

This is obviously a mismatch related to how often organizations update their risk analyses compared to Microsoft's monthly software updates. Microsoft makes its software updates for all its applications along with information about known vulnerabilities, which are made publicly available to all. Microsoft applications and systems, such as Threat Intelligence Tool (Kannavara et al., 2019), are dominant in many organizations, and for these organizations, there will be a need to do RA at least twice per month: (1) publication of the vulnerabilities along with software update (2) then after software update have been installed, so that the vulnerabilities are closed. This initially sounds like an effective solution, but it has several weaknesses. Several of the informants point out that it is challenging to understand the RA when performed by risk analysts, and participation from IT professionals is low in combination with complex IT systems. When we presented the data to the subject matter experts who participated in the survey, they were not surprised.

Kostyuk and Wayne (2021) point to the cyber risk perceptions as the micro-foundations of state cybersecurity. Risk perception is about how individuals and organizations understand, experience, and how to manage cyber risk (Aven, 2015). It is crucial for those involved in RM to have adequate expertise in the field, including those responsible for making risk-related decisions. This involvement ensures effective RM and decision-making processes. To enhance the resilience of a cyber RM system (Section 2.2), organizations should adopt their traditional risk thinking on the basis that cyber risks which are more dynamic and with a high level of uncertainty (*rain from the blue sky ref. fig.2*). In a cyber risk context, the current RM with a systematic approach is not sufficient. RM in organizations should include a systemic risk-based approach, establishing cyber preparedness capable of managing cyber incidents to an acceptable level. A significant characteristic of the systemic perspective is that it considers an organization as "a multi-minded, socio-cultural system, a voluntary association of purposeful members who have come together to serve themselves by serving a need in the environment" (Gharajedaghi, 2011). This implies that the effectiveness of a system depends on a dynamic and non-linear interplay of various functions throughout the entire organization.

Resilience is often discussed in the context of managing risks in complex environments, particularly in situations where there is significant uncertainty associated with the handling of unknown events. As mentioned in Section 2.2, resilience has many definitions, as the term is adapted to different purposes in various fields. This fits well with the responses we received from the informants in our survey when they were asked to describe the concepts of resilience. And according to Engen (Engen et al., 2020), this is due to a lack of understanding of organizations that are, or have been, resilient and that it is difficult to contextualize general theories associated with the concept of resilience.

Erik Hollnagel is referred to by Stavland and Bruvoll (2019) as one of the pioneers within RE. Together with Christopher Nemeth, he has contributed a lot of research within this RE. Their latest resilience definition is simplified compared to previous definitions and is no longer about dealing with unknown incidents related to ensuring security. Hollnagel and Nemeth (2022) emphasize that the resilience definition is more about how an organization or system should handle complexity over time rather than focusing solely on how to recreate the normal situation. As we understand their last definition, the following resilience thinking allows for resilience to be applied in many disciplines in socio-technical systems, which is highly relevant within the cyber domain:

> "*Ability to succeed under varying conditions, so that the number of intended and acceptable outcomes (in other words, everyday activities) is as high as possible"* (Nemeth & Hollnagel, 2022)

In this study, we use the above resilience definition in cybersecurity in a context where a threat actor carries out a cyber-attack with malicious intent in a complex socio-technical system. Determining whether organizations or systems are resilient will then depend on whether they can acceptably handle the cyber-attack. Their behavior related to dealing with the complexity of a cyber-attack will depend on their knowledge based on the normal situation, the cyber-security culture, and the organization's capacities (resilience cornerstones). Establishing and applying resilience functionality in such a consideration will help improve cyber readiness. At the same time, organizations in socio-technical systems that are resilient will also be able to apply the resilience capability in preventive work in IT organizations. This is because resilience is not limited to a specific time perspective.

A resilient organization works continuously and is committed to learning from what is normal, in terms of functionality, on a daily basis, regardless of whether known or unknown changes occur or disturbances.

One method for determining whether organizations or systems are resilient is the "Resilience Analysis Grid (RAG" method (Hollnagel, 2011). The RAG method is beneficial for organizations to assess their resilience level regarding cyber security and devise strategies to enhance their capability to manage unforeseen events. An organization or system is resilient when all four cornerstones (monitoring, anticipating, responding, and learning) are present. Since there are different security cultures in organizations involved in our data gathering, we will use a resilient IT organization as an example when discussing factors of each resilience cornerstone.

An underlying assumption we made here is that as the IT organization gains more experience, they will also enhance their professional competence and become better prepared to recognize what is crucial for maintaining the smooth operation of all the systems under their responsibility. From the end user's perspective, the organization's IT systems will shift from reactive to proactive, thus, more resilient.

5.1 *RAG–- monitor:*

Our findings indicate that effective monitoring requires organizations to clearly understand what needs to be monitored, especially in response to changes, threats, or disruptions. As we understand it, it is about influencing factors that are either present or establishing new factors that or individually contribute to improving the IT organization's monitoring capabilities. In a cyber emergency preparedness perspective, one such factor may be that the IT organization acquires knowledge on how to understand what they should monitor in order to safeguard the companies' values if a cyber incident should occur. To effectively monitor security risks within their scope of responsibility, an IT organization must have a deep understanding of the company's values and overall operations. Another factor may be related to knowledge of suitable technology that meets requirements related to monitoring needs being met. By dimensioning the measures that will handle the monitoring need, the IT organization will also take care of the emergency preparedness needs when this is implemented in the daily IT operations.

However, emergency preparedness in the cybersecurity context has its limits and boundary conditions, as noted by Woods (2018) points to as "brittleness". According to Woods, Brittleness is "a sudden collapse or failure when events push the system up to and beyond its boundaries for handling changing disturbances and variations. By monitoring or measuring the adaptiveness and resilience of the cybersecurity infrastructure, organizations can detect declines in their capacity to adapt to new and evolving threats and take steps to enhance them. Furthermore, the collective knowledge within the IT organization can enhance the organization's monitoring capability. This process includes collective reflection as an individual process to convert tacit knowledge into documents and procedures that are adaptable to the current cyber situation (Patriarca et al., 2021). This continuous process enables the IT organization to improve its monitoring efficiency and targeting.

5.2 *RAG – anticipate:*

Anticipatory awareness, or anticipation, involves the ability to make sense of ongoing changes and collaboratively update the risk picture. To increase relevant knowledge, the cyber security RA should provide a broader risk picture that addresses uncertainty. Sense-making, in the context of this study, is a process in which those who are involved in cybersecurity RM, based on their experiences, understand changes and reflect on what is happening in their circumstances. These reflections, in turn, serve as the primary impetus for taking action (Weick et al., 2005) and establishing redundancy.

An organization's ability to anticipate is dependent on information sharing and the generation of knowledge to understand what to expect, particularly in the event of changes in threats, opportunities, or disturbances. This involves influencing factors that are already present or establishing new factors that individually or collectively contribute to improving the IT organization's predictive abilities. However, On the other hand, some businesses may allocate a significant amount of resources to share information about cyber incidents. From a preparedness perspective, one such factor may be that the IT organization receives sufficient knowledge that will help increase the ability to anticipate the emergency preparedness needs associated with safeguarding the company's values, which will reduce the consequences if a cyber incident should occur. To enhance an IT organization's ability to anticipate potential consequences, it is essential to ensure that they have *operational* knowledge. Another key factor is to increase their understanding of different responses that can help them respond appropriately. The total knowledge within the organization contributes to its ability to predict, and receiving feedback helps in adapting to the current cyber situation.

5.3 *RAG–- respond:*

From a resilience perspective, readiness to respond is about an organization's adaptive capacity, robustness, and rapidity to response in a timely manner. On the one hand, it is important to ensure that the IT organization has the knowledge, processes, and resources to perform daily tasks and to practice emergency preparedness in their area of responsibility. On the other hand, it is important to have resources that can handle a serious cyber incident over an extended period of time.

In a contingency perspective, one response-enabling factor may be that the IT organization receives sufficient knowledge to understand what response is necessary to safeguard the company's values if a cyber incident should occur. With knowledge of what are the organization's values, the IT organization will use this knowledge to understand the importance of implementing relevant emergency response for IT infrastructure, IT systems, computer equipment, and software to reduce consequences related to organizational information security or values in the event of a cyber-attack. By implementing response measures that address emergency preparedness needs, the IT organization can enhance its responsiveness in daily operations. This leads to an improved understanding of response requirements and associated changes or consequences. Additionally, feedback received contributes to the IT organization's overall knowledge, aiding in adapting to current cyber situations.

The ability of the IT organization to continually improve and integrate new knowledge and information, thus reinforcing its capacity to respond with effectiveness and efficiency beyond its boundaries, and augmenting its resilience, aligns with Woods (2018) concept of graceful extensibility.

5.4 *RAG–- learning:*

The ability to learn is about understanding what to learn and how to learn, for example, in the event of changes, threats, or disturbances in an appropriate way. As we understand it, this is about influencing factors that are either present or about establishing new factors that together or individually contribute to improving the learning ability of IT organizations. From a contingency perspective, one such factor may be that the IT organization receives sufficient knowledge to understand what learning is necessary for the organization to be able to safeguard its values if a cyber incident should occur. Learning related to work processes to dimension the IT measures to meet emergency preparedness needs is a factor that will contribute to increased learning in the IT organization. In addition, we can envisage that the total knowledge in the IT organization contributes to feedback on the learning ability of the organization and that this is adapted to the current cyber situation. This is ongoing so that the IT organization's ability to learn becomes more effective and targeted. The other resilience cornerstones receive new information and knowledge that helps improve their capabilities. Debriefing and learning from incidents are valuable sources of learning. To comply with the quality standard ISO 9001:2015, it is necessary to record any findings identified after exercises and incidents in the quality system and analyze them before deciding on and communicating measures throughout the organization. The learning processes primarily involve implementing corrective measures to address identified deviations, which corresponds to what Argyris refers to as single-loop learning (Argyris, 2002).

From the resilience engineering perspective, learning from failures and successes (Hollnagel, 2011) in the context of individuals working together and making sense of their experiences (Deverell, 2021) is at the heart of understanding the operational context. A finding in the survey is related to how the informants encourage reporting of positive and negative events. Around 90% of the respondents somewhat agree that they report negative events, while approximately 50% of the respondents somewhat agree that they don't report positive events. This suggests that reporting positive events may not be as well operationalized in the respondent' organizations.

Learning from day-to-day activities and successful operations should be a continuous and dynamic process facilitated by physical, virtual, cultural, and emotional components, which form a context in motion, known as Nonak's "b" concept. The "b" is a Japanese term that can be translated as a shared space for emerging relationships. The relationship between the knowledge triad promotes a culture of synthesizing both the parts and the whole, integrating the company's strategy with the details of its products through ongoing dialogue and practice (Nonaka et al., 2014). This approach results in a continuous emergence of new knowledge, enhancing resilience in cyber security RM.

6. Conclusion and final remarks

The RAG method employed in this study aimed to investigate the four cornerstones of resilience organizational characteristics: anticipating, monitoring, responding, and learning. Our findings suggest that access to information and learning related to cyber incidents and preparedness varies among informants from different organizations due to the lack of emphasis on cyber security. This results in differing levels of contribution to cyber preparedness improvement. Additionally, our study found that 25% of the companies in our sample only update their cybersecurity risk once a year, which is inadequate given the increasing frequency of cyber-attacks. This failure to regularly update their RA increases the organization' vulnerability to future cyber-attacks. We see similarities between cyber security, RM, and emergency preparedness disciplines. All these topics are relatively new and have evolved significantly over the past few decades. The continuous technological advancements have resulted in increasingly complex IT systems within organizations.

Moreover, there is a growing demand for efficiency and cost reduction, leading to increased outsourcing of IT services. All of this is happening at a time when the threat landscape related to cyber security is changing rapidly. The results of our study indicate an imbalance between the current cyber preparedness of organizations and their desired state, which is due to a lack of expertise and immaturity in the field. To address this, organizations must recognize that cybersecurity is a collaborative effort and involve stakeholders with relevant knowledge and insights to participate in cybersecurity work. This cannot be achieved solely by experts but by those working within the organizations themselves. Furthermore, national and international security situations have contributed to an increased risk of cyber threats, underscoring the importance of strengthening cyber preparedness and security within organizations. Combined with transnational crime, where criminal actors with malicious intentions use cyber technology for their gain, this must be taken more seriously.

The case study is aimed at organizations that have been affected by or have been subjected to a ransom demand, and findings from our study show that they need to strengthen cyber preparedness. We have found that the use of resilience theory enhances cyber business readiness.

To improve cyber readiness, the organization can increase awareness and knowledge of recurrence and focus on what works on a daily basis. This includes developing competence with information security standards, frameworks, and guidelines such as ISO/IEC 27005, NIST 800-30, NIST 800-37, and CIS controls, which can contribute to learning and enhance resilience to create business value. Cyber risks are often viewed as strategic risks that could significantly impact the organization's business. We recommend that senior management and the board increase their focus on cyber risks to address this potential threat.

Many organizations consider cyber risks as strategic risks as they can significantly impact their operations. However, our research revealed that organizational management has not fully recognized the importance of IT as a core business. While organizations are heavily reliant on IT for daily operations, they have not realized that securing IT is also a core business. Study findings indicate that Norwegian organizations have a positive attitude towards IT technology yet struggle to recognize the vulnerabilities it introduces. The study highlights the organization immaturity in understanding cyber technology, leading to surprises when negative cyber events occur. Experts attribute this to a lack of risk understanding, confusion between risk and threat, and a general lack of awareness that cyber security concerns everyone's digital presence.

We recommend that senior management in organizations increase their attention to cyber risk in the future as a core business function. This involves developing a cybersecurity strategy that aligns with the overall organizational strategy, establishing clear roles and responsibilities for cybersecurity, and ensuring all employees are trained and aware of their role in maintaining cybersecurity. Regular cybersecurity RA should be conducted to remain resilient against evolving cyber threats. It is vital for organizations to understand that cybersecurity is not just

an IT issue but a business issue requiring attention and investment at all levels.

References

Argyris, C. (2002). Double-Loop Learning, Teaching, and Research. *Academy of Management Learning & Education, 1*(2): p. 206-218.

Alahmari, A., & Duncan, B. (2020, June). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. *In 2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA)*, pp. 1-5. IEEE.

Aven, T. & Renn, O. (2010). Risk management and governance: *Concepts, guidelines and applications (Vol. 16)*. Springer Science & Business Media.

Aven, T. (2015). *Risikostyring, 2. utgave*, Universitetsforlaget.

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research 253(1)*:1-13.

Aven, T., & Thekdi, S. (2018). The importance of resilience-based strategies in risk analysis, and vice versa. *Domains of resilience for complex interconnected systems.*, pp. 33.

Boin, A., and M. Lodge. 2016. Designing Resilient Institutions for Transboundary Crisis Management: *A Time for Public Administration. Public Administration, 94 (2)*, pp.289–98.

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing octave allegro: *Improving the information security risk assessment process.* Carnegie- Mellon Univ Pittsburgh PA Software Engineering Inst.

Cantelmi, R., Di Gravio, G., & Patriarca, R. (2021). Reviewing qualitative research approaches in the context of critical infrastructure resilience. *Environment Systems and Decisions, 41(3)*, 341-376.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches.* Sage publications.

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: going beyond technical skills for successful cyber performance. *Frontiers in psychology, 9*, 744.

Deverell, E. (2021). *Learning and Crisis, in Oxford Research Encyclopedia of Politics,* W.R. Thompson, Editor. Oxford University Press: Oxford.

Engen, O. A. H., Kruke, B.I., Lindøe, P.H., Olsen, K.H., Olsen, O.E. og Pettersen, K.A. (2020). *Perspektiver på samfunnssikkerhet.* 4. opplag, Capplem Damm Akademisk.

ENISA (2022, 29. July). *ENISA threat landscape for ransomware attacks.* European Union Agency for Cybersecurity. ISBN: 978-92-9204-509-8.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American journal of theoretical and applied statistics, 5(1)*, pp. 1-4.

Ferdinand, J. (2015). Building organizational cyber resilience: A strategic knowledge-based view of cyber security management. *Journal of business continuity & emergency planning, 9(2)*, pp. 185-195.

Force, J. T. (2018). *Risk management framework for information systems and organizations.* NIST Special Publication, 800, 37.

Gharajedaghi, J. (2011). Systems Thinking: Managing Chaos and Complexity: *A Platform for Designing Business Architecture (3. utg.)*. Amsterdam: Elsevier Science.

Henrie, M. (2013). Cyber security risk management in the SCADA critical infrastructure environment. *Engineering Management Journal, 25(2)*, pp. 38-45.

Holling, C. S. (1973). Resilience and stability of ecological systems. Ann. Rev *Ecol System 4(1)*:1–23

Hollnagel, E. (2011). Epilogue: RAG- The Resilience Analysis Grid. In E. Hollnagel, J. Pariès, J. Wreathall, & D. D. Woods (Eds.), *Resilience engineering in practice: A guidebook.* (pp. 275-296). Farnham, UK: Ashgate.

Hollnagel, E. (2018). *Safety-I and safety-II: the past and future of safety management.* CRC press.

Hollnagel, E. (Ed.). (2013). *Resilience engineering in practice: a guidebook.* Ashgate Publishing, Ltd.

Hollnagel, E., & Nemeth, C. P. (2022). *From resilience engineering to resilient performance. Advancing Resilient Performance.* Springer Verlag, pp. 1-9.

Hypponen, M. (2021). *If It's Smart, It's Vulnerable.* Wiley

International Organization for Standardization (2015). *Quality Management Systems—Requirements (ISO standard no. 9001:2015)*

International Organization for Standardization / International Electrotechnical Commission (2018). *Information technology—Security techniques—Information security risk management ISO/IEC standard no. 27005: 2018).*

Kannavara, R., Vangore, J., Roberts, W., Lindholm, M., & Shrivastav, P. (2019, February). A threat intelligence tool for the security development lifecycle. *In Proceedings of the 12th Innovations on Software Engineering Conference* (formerly known as India Software Engineering Conference), pp. 1-5.

Kostyuk, N., & Wayne, C. (2021). The micro foundations of state cybersecurity: *Cyber risk perceptions and the mass public. Journal of Global Security Studies, 6(2)*, ogz077.

Lunde, I.K. (2019). *Praktisk krise- og beredskapsledelse (2. utg.)*. Oslo: Universitetsforlaget, 2019.

Nemeth, C. P. og Hollnagel, E. (2021). *Advancing Resilient Performance.* Springer.

Norwegian Security Act (2018). LOV-2018-06-01-24.

Nonaka, I., Kodama, M., Hirose, A., Kohlbacher, F. (2014). Dynamic fractal organizations for promoting knowledge-based transformation—*A new paradigm for organizational theory. Eur. Manag. J. 32*, 137–146.

Patriarca, R., Falegnami, A., Costantino, F., Di Gravio, G., De Nicola, A., & Villani, M. L. (2021). WaX: An integrated conceptual framework for the analysis of cyber-socio-technical systems. *Safety science, pp. 136*, 105142.

Petruzzi, J., & Loyear, R. (2016). Improving organizational resilience through enterprise security risk management. *Journal of business continuity & emergency planning, 10(1)*, pp. 44-56.

Phillips, R., & Tanner, B. (2019). Breaking down silos between business continuity and cyber security. *Journal of business continuity & emergency planning, 12(3)*, pp. 224-232.

Prior, T., & Hagmann, J. (2014). Measuring resilience: methodological and political challenges of a trend security concept. *Journal of risk research, 17(3)*, pp. 281-298.

Stainton, A., Chisholm, K., Kaiser, N., Rosen, M., Upthegrove, R., Ruhrmann, S., & Wood, S. J. (2019). Resilience as a multimodal dynamic process. *Early intervention in psychiatry, 13(4)*, 725-732.

Stavland, B. & Bruvoll, J.A. (2019). *Resiliense – hva er det og hvordan kan det integreres i risikostyring.* FFI-Rapport 19/00363. Forsvarets forskningsinstitutt.

Steen, R., Ingvaldsen, G., & Patriarca, R. (2021). Engineering resilience in a prison's performance management system. *Safety science,* pp. 142, 105367.

Steen, R. (2019). On the application of the Safety-II concept in a security context. *European Journal for Security Research, 4(2)*, pp. 175-200.

Steen, R., & Aven, T. (2011). A risk perspective suitable for resilience engineering. *Safety science, 49(2)*, pp. 292-297.

Tangenes, T., & Steen, R. (2017). The trinity of resilient organization: aligning performance management with organizational culture and strategy formation. *International Journal of Business Continuity and Risk Management, 7(2)*, pp. 127-150.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). *Organizing and the process of sense-making. 16(4)*, 409-421.

Woods, D. D. (2018). The theory of graceful extensibility: basic rules that govern adaptive systems. *Environment Systems and Decisions, 38(4)*, 433-457.

Works, H. B., & Matters, W. (2023) *How to be a Threat-Centric?*

Øien, K., Jovanovic, A. S., Grøtan, T. O., Choudhary, A., Øren, A., Tetlak, K., ... & Jelic, M. (2017). Assessing resilience of SCIs based on indicators. Smart Resilience Project. European Virtual Institute for Integrated Risk Management, Stuttgart.