EasyChair Preprint

№ 15328

From Uncertainty to Prosecution: Enhancing Cyber Resilience Through Forensic Readiness

Odin Heitmann

October 30, 2024

From Uncertainty to Prosecution: Enhancing Cyber Resilience through Forensic Readiness

Odin Heitmann[1,2][0009−0002−3937−4715]

[1] The National Criminal Investigation Service, Pb. 2094 Vika, 0125 Oslo, Norway
[2] Norwegian University of Science and Technology, Teknologivegen 22, 2815 Gjøvik, Norway
odin.heitmann@politiet.no

Abstract. Organizations relying on digital services must acknowledge that their systems will fail at some point, and if they have not been victims of cybercrime yet, they will be. Cyber resilience is an approach that prepares to withstand and recover from system failures and incidents. To recover from a system failure, the incident's root cause must be understood to mitigate it properly. Thus, there is a need to investigate the incident. An investigation is also essential to hold individuals accountable for malicious incidents in a court of law. The cost of an investigation and the evidential value of digital evidence can depend on how forensically ready an organization is. This apparent connection between cyber resilience and forensic readiness made us question these concepts' interconnection. We conducted a focused literature review and examined relevant legislation, standards, and frameworks to identify the connection between cyber resilience and forensic readiness. Our research shows that the need to determine the root cause of an incident to mitigate it properly is central and that frameworks do not sufficiently address holding individuals responsible for malicious incidents accountable in a court of law. Our main contribution is to show how forensic readiness is a crucial component of cyber resilience and how a systematic investigation is central to understanding the root cause of an incident. We also propose introducing redress as a core function in the NIST Cybersecurity Framework as a first step to ensure criminals are held accountable for their actions.

Keywords: Criminal investigation · Cybercrime · Cybersecurity framework · Cyber resilience · Forensic readiness · Law enforcement · Investigation

1 Introduction

There are two types of organization; i) those that have been victims of cybercrime and ii) those that can be victims of cybercrime. Tjoa et al. [29] refer to a UK study from 2018 that shows that 98% of all UK businesses rely on digital services. In 2023, 99% of enterprises in Norway used ICT [27], and 93,9% of EU enterprises used a fixed broadband connection to the Internet [10]. This means that the majority of businesses in the EU rely on digital services, and they should prepare for their products or systems to become victims of a successful cyberattack or other cyber-related incidents.

Performing traditional risk assessments on an organization's system may have been enough in the past. However, conducting such assessments can be challenging with today's increasingly complex and interconnected systems, and the strategy of hardening systems against known threats may not be enough, as the threat landscape is rapidly evolving [20]. Thus, there is a need for a different approach to prepare for novel threats. One such approach is building *cyber resilience* in the organization. Cyber resilience is to accept that your systems will fail at some point and that you must maintain business continuity even when your systems fail [4].

When a system fails, the next logical step is to mitigate the failure. To apply proper mitigation techniques, the root cause of the failure must be known. An investigation contributes to understanding what and how something has happened, while a criminal investigation aims to stop and prevent criminal activity and to identify individuals behind such activities [13]. Forensic investigations are paramount to determining the root cause of a cyber incident [24], and forensic readiness ensures that organizations can conduct such investigations efficiently by maximizing results with minimal effort [26]. Forensic readiness can enhance cyber resilience by strengthening the overall capability to recover by identifying the root cause.

During our preliminary research, we noticed a notable gap in the literature describing the role of forensic readiness in cyber resilience. To our knowledge, this interconnection has not yet been described. We also noticed that even though investigations are often mentioned as necessary to determine the root cause of incidents, the goal and content of the investigation are not detailed. With this in mind, we defined the following research question to explore the interconnection between forensic readiness and cyber resilience while including the investigative perspective:

Research Question

What is the interconnection between cyber resilience and forensic readiness in the context of preventing and combating cybercrime?

This paper presents fundamentals for cyber resilience, forensic readiness, and investigation before presenting our research on the frameworks, standards, and

legislation that influence cyber resilience. We discuss how forensic readiness contributes to cyber resilience in the context of cybercrime before reflecting on the need to hold inviduals responsible for malicious incidents responsible.

The remainder of the paper is structured as follows. First, we elaborate on our chosen methodology in Section 2. Section 3 provides fundamentals and definitions for cyber resilience, forensic readiness, and investigations. Then, we discuss the results in detail in Section 4 before we reflect on the need to hold individuals responsible for malicious incidents in Section 5. Lastly, we conclude and suggest future work in Section 6.

2 Methodology

To answer the research question, we initially wanted to conduct a literature review only. However, these yielded few results when we conducted keyword searches in Scopus for *("cyber resilience" and "forensic readiness")*. Searching on title, abstract, and keyword, this query only yielded one record, indicating little existing research on the topic.

As the research required insight into cyber resilience as a concept to answer our research question, we decided to use another approach: a multi-stage approach, where we started by obtaining cyber resilience fundamentals before we conducted a focused literature review. Our knowledge of forensic readiness and criminal investigation was derived from the work of Heitmann and Franke [13]

The approach taken in this study was as follows. First, we identified some fundamentals of cyber resilience using the principles of cyber resilience from the World Economic Forum [30], the papers from Björk et al. [4], Linkov and Kott [20], and finally the book from Tjoa et al. [29]. This enabled us to understand the concept of cyber resilience and obtain a starting point for the current relevant standards, frameworks, and legislation.

Then, in April 2024, we conducted a focused literature review using the methodology for literature review proposed by Fink [12]. We used Scopus with the same keyword searches, *("cyber resilience" and "forensic readiness")*, and we searched on all fields. This yielded 29 results. As our final search query included a search in *all* fields, we conducted a full-text review of the 23 records we had access to. We did not apply any exclusion criteria for the full-text review. The rationale for this was to ensure we did not miss any potential linkage between cyber resilience and forensic readiness, as the 23 records would contain references to both cyber resilience and forensic readiness. Our focused literature review focused on the interconnection of cyber resilience and forensic readiness in the context of cybercrime, and we looked for where forensic readiness was described as a part or component of cyber resilience, this being our inclusion criteria. Seven records had implicit connections between cyber resilience and forensic readiness and were included in this study after the full-text review of the 23 records, listed in Table 1a.

After the focused literature review, we read through the standards, frameworks, and legislation listed by Tjoa et al. [29]. When reviewing these docu-

ments, we aimed to identify references to forensic readiness and areas where cyber resilience and forensic readiness interconnect in the context of cybercrime, particularly from a law enforcement perspective. Based on Tjoa et al.'s description of each, the ones that *could* address forensic readiness were chosen to be included in this report. We accessed the standards, frameworks, and legislation by the means presented in Table 1b. Lastly, we synthesized the results and used the results to discuss our findings and answer our research question.

At the end of the research, we realized that redress, i.e., the ability to hold individuals responsible for malicious cyber incidents accountable in a court of law, was missing from cyber resilience and also from the Cybersecurity Framework from the National Institute for Technology and Standards (NIST). Therefore, we chose to discuss the potential inclusion of redress in the final section of this paper.

Table 1: Included literature in this research

(a) Literature review

No.	Paper Title
1	A conceptual redesign of a modelling language for cyber resiliency of healthcare systems
2	AIM Triad: A Prioritization Strategy for Public Institutions to Improve Information Security Maturity
3	Crypto-Ransomware: A Revision of the State of the Art, Advances and Challenges
4	Cyber resilience and incident response in smart cities: A systematic literature review
5	Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis
6	Integrating a Proactive Technique Into a Holistic Cyber Risk Management Approach
7	Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews

(b) Governance frameworks

No.	Legislation/Framework
1	*Digital Operations and Resilience Act* [9]
2	*NIS2* [8]
3	*ISO 22316:2017* [17]
4	*NS-ISO/IEC 27031:2011* [14]
5	*ISO/IEC 27032:2023* [18]
6	*NS-ISO/IEC 27035-1:2016* [16]
7	*NEK ISO/IEC 27035-2:2023* [19]
8	*NIST Cybersec Framework 2.0* [23]
9	*NIST SP 800-53, revision 5* [22]
10	*BSI 200-2* [5]
11	*IT-Grundschutz-Compendium* [11]

3 Fundamentals

This section provides definitions and fundamentals for cyber resilience, forensic readiness, and investigation. Cyber resilience is a comprehensive strategic capability that will be thoroughly defined and explained with clarity to assist readers from various backgrounds in comprehending the concept.

3.1 Cyber resilience

Researchers such as Linkov and Kott have argued that the cyber threat landscape is rapidly evolving, making it clear that hardening systems against known threats is no longer sufficient and that there is a need for a different approach, where one such approach is building *cyber resilience* in the organization [20]. Cyber resilience is comprised of *cyber* and *resilience*. To define *cyber*, we use the definition by the World Economic Forum (WEF), where cyber relates to the interdependent network or information technology infrastructures, including the Internet and computer systems [30]. Linkov and Kott use the definition from

Oxford dictionaries to explain *resilience* in its simplest form as "the capacity to recover quickly from difficulties" [20].

The term *cyber resilience* was introduced at WEF in 2012, and it was then viewed as an additional dimension to cyber risk management [30]. Björk et al. later defined cyber resilience as "the ability to continuously deliver the intended outcome despite adverse cyber events". The key here is to accept that your systems will fail at some point and that you must be able to maintain business continuity even when your systems fail [4]. Linkov and Kott define cyber resilience as "the ability of the system to prepare, absorb, recover, and adapt to adverse effects, especially those associated with cyber attacks.". They also illustrate an example of reliance of a system [20]:

> *Assuming two equally performing systems, A and B, are subjected to an impact (resulting from a cyber-attack) that leave both systems with equal levels of performance degradation, the resilience of system A is greater if after a given period T it recovers to a higher level of performance than that of system B.*

According to Björk et al., the concept of cyber resilience received more attention and usage after it was on the agenda for the WEF in 2012, where WEF created principles and guidelines for risk and responsibility in a hyperconnected world under the heading *Partnering for Cyber Resilience* [4]. WEF emphasized that no organization can address cyber resilience alone. Instead, a collaborative, multi-stakeholder approach is necessary, where even competitors within the same industry must work together as partners to foster a stable and trusted environment. They also point out that future solutions must not focus on the specifics, as these will be quickly outdated. Thus, the solution must have a principle-based approach [30].

Linkov and Kott [20] use the four temporal stages of resilience from the National Academy of Science: i) Prepare, ii) Absorb, iii) Recover, and iv) Adapt, based on Connelly et al. (2017), as illustrated in Figure 1. Time is also highlighted as important, and Linkov and Kott emphasize that cyber resilience revolves around the speed of recovery [20].

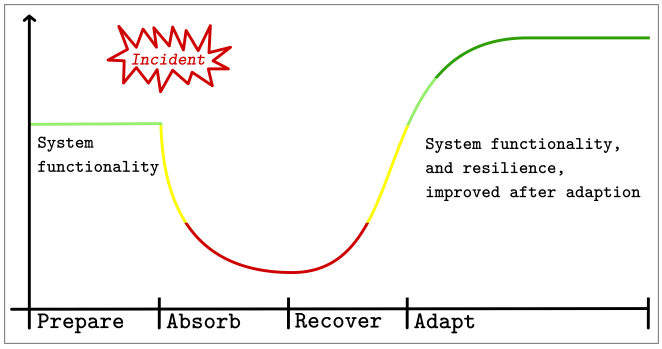

Fig. 1: A system functionality over time, based on Linkov and Kott [20]

In summary, cyber resilience involves the capacity of systems to prepare for, withstand, recover from, and adapt to adverse cyber events by using a holistic approach integrating technical, cognitive, and social aspects. Applied strategies are principle-based, and collaboration across organizations is essential to face evolving cyber threats.

3.2 Digital forensic readiness fundamentals

Tan introduced forensic readiness in 2001 as "the ability to maximize the usefulness of evidence data from incidents while minimizing the cost of forensics during an incident response" [28]. Later, Rowlingson expanded the term to encompass organizations and introduced digital evidence and investigation into the term [26], defining forensic readiness as "the ability of an organization to maximize its potential to use digital evidence while minimizing the cost of an investigation". Rowlingson also described forensic readiness as the knowledge that an incident will occur [26]. Pangalos and Katos introduced the use of controls and how forensic readiness can aid in anticipating disruptive action to operations [25], defining forensic readiness as "the state of the organization where certain controls are in place in order to facilitate the digital forensic processes and to assist in the anticipation of unauthorized actions shown to be disruptive to planned operations".

The UK government's National Technical Authority for Information Assurance (CESG) highlights some risks of not having forensic readiness capabilities in an organization [24]. One such risk is that it is likely that any digital evidence would be lost or unrecoverable after an incident and that it is almost certain it would not be gathered in a way that makes it admissible in a court of law. Another risk is that investigations of incidents would be more challenging to conduct, and it would not be possible to determine the incident's root cause. A lack of forensic readiness reduces learning from previous incidents, thus not supporting future resilience [24].

Heitmann and Franke observed that existing forensic readiness models overlook the significance of addressing the investigative requirements of law enforcement, representing a deficiency in incident responses that transition into a criminal investigation [13]. They argued that forensic readiness falls short of capturing the essential cross-organizational preparedness and the ability to prevent, mitigate, and prosecute cybercrime. As a solution, they advocated introducing criminal investigation integration as a new component of future forensic readiness models to ensure the fulfillment of criminal investigation needs.

Heitmann and Franke also proposed the term *cross-organizational investigative readiness* to describe how relevant stakeholders across various organizations must prepare for future forensic criminal investigations and collaboration to ensure that applied methodology and handling of potential digital evidence makes is usable both for incident response, as well as for criminal investigations in cases where incidents escalate to such investigations [13].

In summary, forensic readiness includes proactive planning and preparation for investigating cyber incidents. It aims to maximize an organization's ability

to use digital evidence while minimizing the cost of an investigation. However, it does not sufficiently address law enforcement's criminal investigative requirements and needs.

3.3 Investigation fundamentals

The literature in our focused review often mentions investigations, but the definition of an investigation is not clearly stated. Therefore, in this section, we will outline our understanding of the fundamentals of an investigation.

The term *investigation* refers to a methodical and comprehensive process of collecting, analyzing, and assessing information, evidence, and facts to uncover and comprehend the details surrounding a specific event, situation, or circumstance. This can be achieved by seeking answers to the 5WH questions [1,2,15], shown in Fig 2 below.

The 5WH formula

What happened? When did it occur? Where did it happen? Who was involved? Why did it happen? How did it happen?

Fig. 2: The 5WH formula, outlining key questions for analysis, from Årnes [1]

The differentiation between an investigation and a *criminal* investigation depends on the conducting authority and the objective. An investigation may occur within an organization, with or without suspicion of criminal behavior, to find the cause behind a problem or challenge, whereas a criminal investigation is generally carried out by law enforcement to prevent and stop criminal activity [13].

4 Discussion

Our research aimed to explore the relationship between cyber resilience and forensic readiness in the context of preventing and combating cybercrime, as little to no such research exists on this topic to the best of our knowledge. Despite conducting a thorough scoped literature review and examining relevant legislation, standards, and frameworks, we found no explicit interconnection between cyber resilience and forensic readiness. However, based on our professional experience with digital forensics and cyber crime investigation, we identified several implicit connections between cyber resilience and forensic readiness that warrant further exploration.

One recurring topic found in this focused review is the need to determine the cause of the incident to mitigate it [3,9,22]. To uncover and comprehend the cause of an incident, an appropriate investigation should be conducted [11]. As

pointed out by CESG [24], investigations of incidents will be more challenging without forensic capabilities, and without such capabilities, it will be impossible to determine the root causes of incidents. Failure to uncover and understand the root cause of an incident without answering the questions from Figure 2 leads to guessing details related to the incident, rendering the incident response less effective and, most likely, more costly.

To establish the implicit connections between cyber resilience and forensic readiness as an interconnection and to support our line of reasoning, we, therefore, need to assume the following prerequisite:

To truly understand the root cause of a cyber incident, an investigation must be conducted

Fig. 3: The necessity of investigations while determining cyber incident causes

Using a forensic approach during the investigation can ensure that the collected, preserved, and analyzed data is usable later in a court of law or for legal matters [24]. Thus, the desired approach for an organization should be to be forensically ready to investigate an incident to understand the root cause of a cyber incident as quickly as possible to mitigate it faster and cheaper. A positive side effect is that data collected using forensic principles during an incident can be used at later stages, i.e., in a court of law or for other legal matters.

Following the line of reasoning above, we have established a connection between the need to understand the root cause of a cyber incident by investigating it and how forensic readiness contributes to this investigation. Forensic readiness also contributes to the effectiveness of incident mitigation, as well as ensures the data's admissibility in a court of law or for legal matters at a later stage. This enables us to discuss the potential interconnections between cyber resilience and forensic readiness found in our focused literature review and examination of legislation and standards.

The remainder of this section is based on the four phases of cyber resilience by Linkov and Kott [20], illustrated in Fig. **??**; i) Prepare, ii) Absorb, iii) Recover, and iv) Adapt. Using these phases, we aim to provide the reader with a clear understanding of how forensic readiness interconnects with cyber resilience throughout the process.

The preparation phase is essential for an organization's cyber resilience and forensic readiness. It lays the groundwork for future investigations and the organization's overall ability to handle cyber incidents. Introducing cyber resilience and forensic readiness in the organization will require allocating resources through funding and effort from various departments, thus requiring top management support. The organization's top management should initiate the

preparation phase, as they are responsible for initiating, controlling, and monitoring the security process [5].

Cyber resilience and forensic readiness concepts can be developed after performing a structural analysis of the organization, where the business processes and their corresponding tasks are gathered, based on the approach to create a security concept from BSI [5]. Asset management and knowing the organization's topology can give organizations more structure in protecting their assets and increase the time to identify and collect potential digital evidence. This can reduce the cost of the investigation by providing an overview of the assets and topology from the offset of an incident. Creating this baseline overview of the organization's topology of systems is never finished as evolving systems change. Thus, this overview should be continuously updated to reflect the current topology [22].

During the preparation phase, various frameworks and standards can aid in building the organization's cyber resilience and forensic readiness capabilities.

The National Institute of Standards and Technology (NIST) released version 2.0 of their Cybersecurity Framework (CSF) [23] in 2024, aiming to guide industry, government agencies, and other organizations in managing cybersecurity risks. The CSF describes desired outcomes intended to be understood by a broad audience, e.g., executives, managers, and practitioners, regardless of their cybersecurity expertise. The outcomes are generalized and not specific to any sector, country, or technology. Thus, the organizations using the framework have the flexibility to use it for their particular risks, technologies, and business models. The outcomes are mapped to a list of potential security controls, enabling a quick way to mitigate cybersecurity risks.

The CSF framework consists of three main parts: i) Core, ii) Organizational Profiles, and iii) Tiers. The **core** consists of a taxonomy with high-level security outcomes and consists of six functions, *Govern, Identify, Protect, Detect, Respond, and Recover* as shown in Fig. 4a. Using the framework, an organization can enhance its cyber resilience in various domains, focusing on the functions in the framework. To illustrate how the six functions relate, the CSF can be viewed as a wheel, as shown in Fig. 4b. The *respond* function relates to incident handling, thus addressing the need for an investigation to determine the root cause of an incident. Having forensic readiness capability as part of the CSF can strengthen the organization's overall cybersecurity posture and cyber resilience.

ISO 27031 recommends that critical ICT services are identified and documented, including how they are configured or linked [14]. An inventory of relevant assets such as information systems, applications and databases, and hardware and software systems should be present in the ICT response and recovery plan documentation [14]. Such inventory must be sufficient for tracking and reporting [22]. Management of new installs can include an overview of where and when what kind of software is installed, making the investigation easier later on if a specific type of software is attacked or if a vulnerability is discovered. Keeping an updated inventory of hardware, software, and processes can also enable the investigation to target its scope [8].

Function	Category
Govern (GV)	Organizational Context
	Risk Management Strategy
	Roles, Responsibilities, and Authorities
	Policy
	Oversight
	Cybersecurity Supply Chain Risk Management
Identify (ID)	Asset Management
	Risk Assessment
	Improvement
Protect (PR)	Identity Management, Authentication, and Access Control
	Awareness and Training
	Data Security
	Platform Security
	Technology Infrastructure Resilience
Detect (DE)	Continuous Monitoring
	Adverse Event Analysis
Respond (RS)	Incident Management
	Incident Analysis
	Incident Response Reporting and Communication
	Incident Mitigation
Recover (RC)	Incident Recovery Plan Execution
	Incident Recovery Communication

(a) NIST CSF Core functions and categories, by [23]

(b) Cyber Functions Wheel, by [23]

Fig. 4: Cyber Functions Wheel and NIST CSF Core Functions

ISO 22316 addresses principles and attributes for building organizational resilience [17], emphasizing the importance of absorbing and adapting to the impact of sudden and unexpected incidents and preparing to respond effectively to change. Appropriate resources and the capacity to respond to incidents are also imperative to cyber resilience [17]. As described at the beginning of this section, forensic readiness can aid the investigation in determining the root cause of an incident. Thus, by implementing the ISO 22316 standard to build organizational resilience, forensic readiness capability should be available to support investigations.

ISO 27035-1 describes incident management principles [16], underlining the need to understand that security policies or controls alone will not guarantee total protection against incidents. Due to this, it is necessary to prepare to deal with incidents, as failing to prepare can lead to a less effective response and increase the potential impact of the incident. According to the standard, the organization must have a structured and planned response to incidents and appropriate controls to prevent, reduce, and recover from impacts caused by the incident [16]. As described in Section 3, an investigation is a methodological approach to uncovering and comprehending details surrounding an incident, and forensic readiness contributes to the investigation by reducing the cost of the investigation and maximizing the results.

The BSI 200-2 standard involves business continuity management and describes how contingency planning can reduce the impact of an incident and thereby secure operations [5]. This planning should contain information about roles, immediate measures, and restoration plans [5], supporting the need for an organization to have forensic readiness capability available to mitigate inci-

dents, reduce their impact, and recover. The investigation's results can be used to prevent new incidents within the organization or for external collaborative organizations.

Incident handling capability is essential to cyber resilience. NIST SP 800-53r5 describes the implementation of such capability according to an incident response plan [22]. ISO 27032 and BSI 200-2 recommend establishing an incident management team to enable the organization to assess, respond to, or learn from incidents [18,5]. BSI 200-2 further suggests that the organization has a procedure for handling security incidents and an escalation strategy detailing who will be involved in what way and when for different types of incidents [5]. Such escalation strategy can involve other stakeholders, e.g., can law enforcement be a relevant stakeholder if the nature of the incident is criminal. The recommendation to have an incident handling capability in the organization is not only found in these three standards. Even though it is only mandatory for financial entities in the European Union, the Digital Operational Act states that financial entities must be capable of handling *all* ICT-related incidents [9]. Using the prerequisite that an investigation needs to be conducted to identify the root cause of an incident by using a forensic approach implies that the financial entities must have such capabilities available before an incident occurs. Part of their cyber resilience thus relies on having forensic readiness capability available to support an investigation of incidents.

Potential digital evidence will be collected during the incident handling. It is, therefore, necessary to prepare to collect this evidence. BSI 200-2 recommends creating a guide on securing evidence, including procedures, technical tools, and documentation requirements [5]. ISO 27032 recommends that organizations define and apply procedures for identifying, collecting, acquiring, and preserving information that can be used as evidence. It is clearly stated that evidence is expected to be collected in a manner that makes it admissible in a court of law. Hence, organizations must gather the necessary information for future use in legal proceedings or a court of law [18]. In ISO 27035-2, it is presupposed that evidence indeed is collected in a manner that makes it admissible in a court of law, showing that the collected records are complete and have not been tampered with in any way and that copies of electronic evidence are identical to the original data source [19]. Following forensic principles during the incident response as part of an investigation will thus contribute to ensuring that evidence is admissible.

Logs are one of the digital forensics investigations' most used information sources, according to Casino et al. [6]. Logs can also be used to determine malicious activity and contribute to answering the 5HW questions. Thus, to support investigations, organizations should facilitate logging relevant data as part of their forensic readiness. ISO 27032 recommends that logs recording activities, exceptions, faults, and other relevant events are produced, protected, kept, and analyzed. Such logs should be kept securely for log analysis and audit [18]. Secure storage of logs can contribute to maintaining the evidentiary value. ISO 27035-1 recommends that system and network activity is monitored and logged

[16]. NIST recommends that event types that are logged are accompanied by a rationale for selecting these event types and information on how the events can support the investigation of incidents [22]. The event record must contain, as a minimum, the following information: i) What type of event, ii) when the event occurred, iii) where the event occurred, iv) the source of the event, v) the outcome of the event, and vi) identities related to the event [22]. The information in these event records contributes to answering the 5HW questions, at least for the particular event. Finally, in the 200-2 standard from BSI [5], it is recommended that all relevant data is collected securely and stored to make it usable for later evaluation. The collected data should be filtered, normalized, aggregated and correlated, and ready for assessment [5].

Absorption phase This phase begins when the incident occurs, though it can take some time before it is discovered. Marotta and McShane [21] refer to an IBM/Ponemon study from 2017, where the mean time to become aware of a breach was 191 days. Notably, organizations that identified the breach earlier had a significantly lower total cost related to the incident than organizations with delayed discovery [21]. When the incident is revealed, an incident response should be initiated to confirm the nature and extent of the incident and to contain it [14]. During incident response, an investigation is typically conducted to ensure an appropriate response and support forensics and recovery activities [23]. The investigation can guide the categorization of the incident, and forensic analysis, as a part of the investigation, aids the incident classification, prioritization, and assessment of the damage [3]. The incident needs to be quickly identified, and vulnerabilities in network and information systems must be remedied to reduce risk [8].

An incident handler should assess to determine if the event is a possible or confirmed incident or if the event is a false alarm [16]. The BSI 200-2 standard recommends deciding whether to contain the damage or resolve the incident, depending on what is more important [5]. To make this assessment, the incident handler must at least seek preliminary answers to the 5WH questions. Revisiting Tan's original definition of forensic readiness from [28], the goal is to maximize the usefulness of evidence data from incidents while reducing the cost during incident response. Thus, this initial assessment can be more straightforward if the organization and the incident handler are forensically ready. The incident handlers should not make this decision alone but according to the person in charge and the organization's incident response plan. If there is a possibility that the incident is criminal in nature, law enforcement could also be consulted. This is especially beneficial if the incident indeed is of a criminal nature, and law enforcement needs to take charge of the investigation at a later stage.

Reporting is an essential part of incident response. ISO 27035-2 provides examples of incident reports. The information that shall be filled out answers what/how/why it occurred, along with a description of the initial view of components and assets affected, and the adverse business impacts [19]. These questions are relatable to the 5HW questions used in investigations.

Recovery phase As described in the absorption phase, a proper incident response can lead to a more efficient recovery and minimize downtime. Answers to the 5HW can determine which systems are affected and in what way, and it eliminates guessing. This can speed up recovery time, but it relies on knowing the true root cause of the incident. Thus, there is a need for an investigation in the recovery phase.

Adaption phase The final phase in cyber resilience is the adaption phase. In this phase, lessons learned from incident handling can be used to improve the system's functionality and increase its resilience. The Digital Operation Resilience Act states that post incident reviews after *major* incidents are required to identify operations or business continuity policy improvements. One aspect to be covered in the post incident review is the quality and speed of the forensic analysis [9]. This requires truly understanding the root cause, and if the approach has been ad-hoc without proper documentation, the review would have limited value as it will be hard to backtrack on what has happened without answering the 5HW questions.

5 Cyber resilience from a law enforcement perspective

Comparing cybercriminals with terrorists, Marotta and McShane underline the fact of the asymmetric information advance the cybercriminals have, where the cybercriminals only need to get things right once, while the defenders need to be right every time [21]. From a law enforcement perspective, this can be argued to be reversed. Law enforcement only needs to be lucky once, while cybercriminals must cover their tracks perfectly every time. But for this to work in practice, law enforcement is dependent on admissible and reliable evidence. Thus, organizations must have proper cyber resilience and forensic readiness to collect such evidence during their investigation of incidents that later escalate to criminal investigations.

Heitmann and Franke found that forensic readiness did not sufficiently cover the criminal investigative perspective and that various stakeholders *industry, incident response teams*, and *law enforcement* had conflicting interests during a cyber attack [13]. Hence, they proposed integrating criminal investigation into forensic readiness strategies and models to ensure that the criminal investigative perspective is not overlooked.

Heitmann and Franke also highlighted the absence of a *redress* strategy in forensic readiness [13]. As defined by Endicott-Popovsky and Frincke [7], redress is the ability to hold intruders accountable in a court of law and the ability to retaliate. During our focused literature review and examination of standards and legislation, we were unable to find any emphasis on redress. We find it quite surprising that this crucial focus is consistently absent, considering that holding individuals accountable can help prevent future incidents. When looking at the functions of NIST CSF in Section 4, it becomes apparent that it lacks an outcome to hold the individuals behind malicious incidents accountable. Thus,

we propose that *redress* is added as a core function in the CSF to emphasize the importance of holding individuals responsible for such incidents accountable for their actions. By beginning with the CSF from NIST [23], we aim to raise awareness that future cyber resilience research, frameworks, and standards must recognize the importance of redress in preventing and combating cybercrime.

6 Conclusion and future work

Cyber resilience enhances the organization's ability to maintain operational continuity during and after an incident. The interconnection between cyber resilience and forensic readiness is that forensic readiness helps answer the 5WH questions during an investigation, which is necessary to determine the root cause of an incident. After determining the root cause of an incident, the organization can address the incident with an appropriate mitigation response, thereby supporting and maintaining operational continuity by either removing or reducing the impact. Forensic readiness also ensures that the organization is prepared to collect, analyze, and preserve potential digital evidence after an incident, making the evidence admissible in a court of law or usable for legal matters, thus supporting law enforcement in investigating malicious incidents.

This research is exploratory and does not encompass all aspects of cyber resilience and forensic readiness. The aim was to examine the interconnection between cyber resilience and forensic readiness, serving as a starting point for further research and discussion of this interconnection. An important point that deserves more study and discussion is that an incident instigated by malicious individuals is not concluded once the incident is resolved. The individuals responsible for such incidents must be held accountable in a court of law. Upcoming studies could focus on adopting forensic readiness into cyber resilience strategies to highlight forensic readiness as an integral part of cyber resilience. Studies could also research integrating redress in cyber resilience strategies to uphold the law enforcement perspective.

Acknowledgments. This research was funded, in whole or in part, by The Research Council of Norway [338691]. For the purpose of open access, the author has applied a CC BY public copyright license to any Author Accepted Manuscript (AAM) version arising from this submission. The author extends sincere gratitude to Professor Katrin Franke for invaluable guidance and support in shaping the focus of this research and to Dr. Jan William Johnsen for providing valuable feedback to the manuscript.

References

1. Årnes, A.: Digital forensics. John Wiley & Sons (2017)
2. Årnes, A.: Introduction. In: Årnes, A. (ed.) Cyber Investigations, pp. 1–12. John Wiley & Sons (2023)
3. Athinaiou, M., Mouratidis, H., Fotis, T., Pavlidis, M.: A conceptual redesign of a modelling language for cyber resiliency of healthcare systems. In: Katsikas, S., Cuppens, F., Cuppens, N., Lambrinoudakis, C., Kalloniatis, C., Mylopoulos, J.,

Antón, A., Gritzalis, S., Pallas, F., Pohle, J., Sasse, A., Meng, W., Furnell, S., Garcia-Alfaro, J. (eds.) Computer Security. pp. 140–158. Springer International Publishing, Cham (2020)
4. Björck, F., Henkel, M., Stirna, J., Zdravkovic, J.: Cyber resilience – fundamentals for a definition. In: Rocha, A., Correia, A.M., Costanzo, S., Reis, L.P. (eds.) New Contributions in Information Systems and Technologies, Advances in Intelligent Systems and Computing, vol. 353, pp. 311–316. Springer International Publishing, Cham (2015). https://doi.org/10.1007/978-3-319-16486-1_31
5. Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz methodology. Tech. Rep. 200-2, Bundesamt für Sicherheit in der Informationstechnik (2017), https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.pdf?__blob=publicationFile&v=2, accessed: 2024-08-24
6. Casino, F., Dasaklis, T.K., Spathoulas, G.P., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M., Patsakis, C.: Research trends, challenges, and emerging topics in digital forensics: A review of reviews. IEEE Access **10**, 25464–25493 (2022). https://doi.org/10.1109/ACCESS.2022.3154059
7. Endicott-Popovsky, B., Frincke, D.: Adding the fourth "R" [CERT's model for computer security strategies]. Proceedings from the Fifth Annual IEEE System, Man and Cybernetics Information Assurance Workshop, SMC p. 442 – 443 (2004)
8. European Parliament and Council: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 december 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (2022), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555, last accessed: 2024-08-09
9. European Parliament and Council: Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 december 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (2022), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554, last accessed: 2024-08-09
10. Eurostat: Digital economy and society statistics - enterprises (2023), https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_enterprises#Access_to_the_internet, accessed: 2024-09-23
11. Federal Office for Information Security: IT-Grundschutz-Compendium. Tech. Rep. 200-2, Bundesamt für Sicherheit in der Informationstechnik (2017), https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2022.pdf?__blob=publicationFile&v=2, accessed: 2024-08-26
12. Fink, A.: Conducting research literature reviews: From the internet to paper. Sage publications (2019)
13. Heitmann, O., Franke, K.: Exploring digital forensic readiness: A preliminary study from a law enforcement perspective (2023), https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3125648
14. International Organization for Standardization: Information technology security techniques guidelines for information and communication technology readiness for business continuity. ISO Standard NS-ISO/IEC 27031:2011, ISO (2015), https://online.standard.no/nb/ns-isoiec-27031-2011

15. International Organization for Standardization: Information technology — security techniques — incident investigation principles and processes. ISO Standard ISO 27043, ISO (2015), https://www.iso.org/standard/44407.html
16. International Organization for Standardization: Information technology security techniques information security incident management part 1: Principles of incident management. ISO Standard NS-ISO/IEC 27035-1:2016, ISO (2018), https://online.standard.no/nb/ns-isoiec-27035-1-2016
17. International Organization for Standardization: Security and resilience — organizational resilience — principles and attributes. ISO Standard ISO/IEC 22316:2017, ISO (2020), https://online.standard.no/nb/ns-iso-22316-2017
18. International Organization for Standardization: Cybersecurity — guidelines for internet security. ISO Standard NEK-ISO/IEC 27032:2023, ISO (2023), https://online.standard.no/nb/nek-isoiec-27032-2023
19. International Organization for Standardization: Information security incident management part 2: Guidelines to plan and prepare for incident response. ISO Standard NEK ISO/IEC 27035-2:2023, ISO (2023), https://online.standard.no/nb/nek-isoiec-27035-2-2023
20. Linkov, I., Kott, A.: Fundamental concepts of cyber resilience: Introduction and overview. In: Kott, A., Linkov, I. (eds.) Cyber Resilience of Systems and Networks, pp. 1–25. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-319-77492-3_1
21. Marotta, A., McShane, M.: Integrating a proactive technique into a holistic cyber risk management approach. Risk Management and Insurance Review **21**(3), 435–452 (2018). https://doi.org/https://doi.org/10.1111/rmir.12109, https://onlinelibrary.wiley.com/doi/abs/10.1111/rmir.12109
22. National Institute of Standards and Technology: Security and privacy controls for information systems and organizations. Tech. Rep. NIST SP 800-53, Rev. 5, National Institute of Standards and Technology (2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf, accessed: 2024-04-29
23. National Institute of Standards and Technology: The NIST cybersecurity framework (CSF) 2.0. Tech. Rep. NIST CSWP 29, National Institute of Standards and Technology (2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf, accessed: 2024-04-29
24. National Technical Authority For Information Assurance: Good practice guide forensic readiness **1.2** (2015)
25. Pangalos, G., Katos, V.: Information assurance and forensic readiness. In: Next Generation Society. Technological and Legal Issues: Third International Conference, e-Democracy 2009, Athens, Greece, September 23-25, 2009, Revised Selected Papers 3. pp. 181–188. Springer (2010)
26. Rowlingson, R.: A ten step process for forensic readiness. International Journal of Digital Evidence **2**(3), 1–28 (2004)
27. Statistics Norway: Use of ICT in business (2023), https://www.ssb.no/en/teknologi-og-innovasjon/informasjons-og-kommunikasjonsteknologi-ikt/statistikk/bruk-av-ikt-i-naeringslivet, accessed: 2024-09-23
28. Tan, J.: Forensic readiness. Cambridge, MA:@ Stake **1** (2001)
29. Tjoa, S., Gafić, M., Kieseberg, P.: Cyber resilience fundamentals. Springer International Publishing (2024), https://books.google.no/books?id=OTJi0AEACAAJ
30. World Economic Forum: Partnering for cyber resilience. Risk and responsibility in a hyperconnected world - principles and guidelines. Tech. rep. (2012), https://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf, accessed 2024-04-15