sustainability

MDPI

Concept Paper

Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity

Muhammad Fakhrul Safitra [1], Muharman Lubis [1,*] and Hanif Fakhrurroja [1,2,*]

[1] School of Industrial Engineering, Telkom University, Bandung 40257, Indonesia; fakhrulsafitra@student.telkomuniversity.ac.id
[2] National Research and Innovation Agency, Jakarta Pusat 10340, Indonesia
* Correspondence: muharmanlubis@telkomuniversity.ac.id (M.L.); haniff@telkomuniversity.ac.id (H.F.); Tel.: +62-821-1693-4452 (M.L.); +62-818-647-004 (H.F.)

Abstract: Amidst the rapid advancements in the digital landscape, the convergence of digitization and cyber threats presents new challenges for organizational security. This article presents a comprehensive framework that aims to shape the future of cyber security. This framework responds to the complexities of modern cyber threats and provides guidance to organizations to enhance their resilience. The primary focus lies in the integration of capabilities with resilience. By combining these elements into cyber security practices, organizations can improve their ability to predict, mitigate, respond to, and recover from cyber disasters. This article emphasizes the importance of organizational leadership, accountability, and innovation in achieving cyber resilience. As cyber threat challenges continue to evolve, this framework offers strategic guidance to address the intricate dynamics between digitization and cyber security, moving towards a safer and more robust digital environment in the future.

Keywords: cyber resilience; digitalization capabilities; cybersecurity; threats and risks; preparedness; adaptability; incentivizing stakeholders; framework

Citation: Safitra, M.F.; Lubis, M.; Fakhrurroja, H. Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability* **2023**, *15*, 13369. https://doi.org/10.3390/su151813369

Academic Editor: Harris Wu

Received: 22 July 2023
Revised: 30 August 2023
Accepted: 31 August 2023
Published: 6 September 2023

1. Unifying the Concept of Resilience

The concepts of capability and resilience have become increasingly important in various business aspects in recent years [1,2]. Alongside the growing awareness of environmental and social impacts, businesses now better understand the necessity of integrating principles of capability and resilience to meet consumer expectations and ensure long-term operational sustainability. A strong indicator of this shift is evidenced by research conducted by Nielsen, revealing that approximately 66% of consumers worldwide are willing to pay a higher premium for products and services that demonstrate commitment to the environment and society. This reflects a consumer behavioral shift that increasingly values products that provide not only quality but also positive impacts on the environment and society.

Perceptions of resilience have also undergone transformation. The World Economic Forum indicates that resilience has risen to become one of the top five risk trends the world will face in 2022. This signifies that businesses must not only tackle day-to-day challenges but also possess the capability to adapt and endure in the face of rapid and unforeseen changes within the dynamic global environment.

Thus, the shift toward the concepts of capability and resilience is not merely a passing trend; rather, it has become a crucial pillar in successful business strategies. Businesses that can effectively integrate these aspects into their operations will have greater opportunities to win consumer favor, navigate complex challenges, and sustain long-term growth in an ever-changing world.

Table 1 provides a comprehensive visualization of the cybersecurity concept aimed at elucidating and comprehending various critical aspects related to cyber protection and threat mitigation.

Table 1. Synergy of cybersecurity, digitization capability, sustainability, and resilience concepts in business.

No	Topic	Description	Importance	Implementations
1.	Cybersecurity Measures and Best Practices	Describing the importance of implementing cybersecurity measures and best practices such as data encryption, strong authentication, rigorous network monitoring, and security training for end-users. The goal is to build a system that possesses robust security and can withstand increasingly complex cyber threats.	Preventing unauthorized access, reducing the risk of data leakage, and safeguarding system integrity.	- Implementation of end-to-end encryption for sensitive communications. - Implementation of multi-factor authentication for system access.
2.	Collaborative Information Sharing	Highlighting the importance of cross-organizational, governmental, and other stakeholder collaborations in facing cyber threats. This involves the exchange of information about ongoing threats, successful mitigation strategies, and the latest developments in the cybersecurity domain. By sharing information, the involved entities can collectively identify, analyze, and address threats more effectively.	Enabling early detection of new threats, enhancing understanding of attack trends, and reducing the impact of attacks.	- Cross-industry cyber threat intelligence sharing platform. - Collaborative forum between government and industry.
3.	Various Aspects	Summarizing various aspects contributing to the concept of resilience in general. This encompasses system flexibility in facing disruptions, recovery after incidents, operational sustainability under challenging conditions, and adaptation to dynamic environmental changes. These aspects collectively form the foundation for maintaining operational continuity in the face of challenges, including cyber threats.	Ensuring the organization continues to operate even in the event of disruptions or major incidents.	- Disaster recovery planning involving IT systems. - Utilization of cloud architecture for scalability.
4.	Digitalization Capabilities	Explaining the importance of digitization capabilities in confronting challenges of the digital era, including the integration of new technologies, adaptation of business models, and digital-based innovation.	Enhancing operational efficiency, competitiveness, and the ability to adapt to technological changes.	- Implementation of IoT for real-time monitoring in industries. - Utilization of data analytics for decision-making.
5.	Sustainability and Resilience	Demonstrating the significance of sustainability and resilience concepts in tackling modern challenges. As customers increasingly prioritize sustainable products and services and with the presence of increasingly complex threats, sustainability and resilience become key elements in business strategies.	Enhancing customer loyalty, reducing operational risks, and maintaining business continuity.	- Utilization of renewable energy in the supply chain. - Development of sustainable plans for risk mitigation.

There are numerous reasons why businesses need to consider capability and resilience. First, it is a moral issue. Businesses have a responsibility to manage natural resources wisely and reduce their impact on the environment. Second, capability and resilience can save businesses money; for example, businesses that use renewable energy can reduce their energy bills [3]. Third, capability and resilience can enhance a business's reputation. Consumers are increasingly seeking socially and environmentally responsible businesses. Designing a system to improve what is referred to as cybersecurity resilience is an area of prominent study [4,5]. Companies must currently balance meeting market expectations

regarding competitiveness with maintaining their operational capability economically, environmentally, and socially [6,7]. Maintaining capability and resilience in the community within the current environment is an essential component of corporate strategy and competitiveness [8,9]. Recent study findings indicate that the potential offered by a company's digitization capability is one of the most viable options to address these critical demands. Specific examples of how digitization capability can assist companies in meeting these critical demands include:

- Digitization capability can help companies enhance efficiency through automating manual tasks and integrating business processes. This can reduce the time and cost required to complete specific tasks and enhance the accuracy and consistency of work outcomes.
- Digitization capability can help companies increase revenue by expanding their market, developing new products and services, and enhancing customer satisfaction. This can be achieved by leveraging digital technology to reach new customers, understand their needs and preferences, and provide solutions that align with these requirements.
- Digitization capability can help companies enhance competitiveness by providing them access to broader information and resources, enabling faster innovation. This can be achieved by leveraging technologies such as big data, analytics, and machine learning to gather and analyze data and generate insights that can be used to develop more effective business strategies.

Overall, digitalization capability is a crucial avenue for companies confronting the challenges of the current digital era. By effectively leveraging digital technology, companies can enhance their efficiency, revenue, and competitiveness, as well as prepare themselves to face future challenges.

The strategies and operations of companies have been significantly influenced by the growth of digitization capability [10,11]. A study by the International Data Corporation (IDC) found that the digital technology market will reach USD 2.1 trillion by 2023. Involvement in digital consumers has enabled businesses in various industries to provide a better user experience [12,13]. However, cyberattacks are increasingly frequent due to the complexity of the digitized cyber environment. A report by Cybersecurity Ventures estimated that the global economic cost of cyberattacks will reach USD 10.5 trillion by 2025. While digitization capability offers many benefits, it also makes businesses more vulnerable to sophisticated cyber threats. Consequently, the concept of "cyber resilience with digitization capability", which describes an organization's capacity to anticipate, prepare for, respond to, recover from, and adapt to cyberattacks, has become significant [14,15]. For companies, effective cybersecurity management has become crucial. There is a trade-off between the benefits of such expenditures and the economic capability of the organization [16]. Investing in cybersecurity and digitization provides several benefits. Given limited resources, small and medium-sized businesses (SMEs) must carefully consider the extent of their investment in this field [17].

A company's ability to utilize digital networks, business resources, and assets to leverage opportunities and drive innovation in products, services, and procedures is known as digitization capability [18,19]. Through organizational learning, customer value generation, and innovation management, this capability is considered crucial for gaining long-term competitive advantage. We are aware that despite the growing interest in this topic, there are few contributions that explore digitization capability and its relationship with cyber resilience. To fully understand how digitization capability influences cyber resilience, this research will conduct an in-depth investigation.

We have conducted a comprehensive review of recent literature on theories and frameworks for digitization capability, cyber resilience, and their relationship [20,21]. Based on recent developments in digitization capability and cybersecurity management, we present a more in-depth conceptual framework to understand the relationship between these two concepts. We explain how digitization capability can help enhance cyber resilience by demonstrating that digitization capability is involved in the planning/preparation

and adaptation stages of the cyber resilience process. Online information capability can drive both of these stages, while other capabilities such as diversified resource utilization and the promotion of continuous learning can drive the planning/preparation stage. On the other hand, scanning the evolution of the digital environment and timely resource reconfiguration can drive the adaptation stage.

Research Questions:

RQ1:	What is the relationship between digitization capability and cyber resilience in the digital era?
RQ2:	What are the key factors shaping an organization's cyber resilience against cyberattacks?
RQ3:	How do various digitization capabilities contribute to strengthening the phases of cyber resilience?
RQ4:	How can continuous research and development enrich the cyber resilience framework amid constant changes in the digital ecosystem?

This research aims to investigate the influence of capability and resilience concepts on the business world, with a focus on the moral role, economic benefits, and reputation within the context of these concepts. Additionally, this research aims to analyze the impact of the growth of digitization capability on company strategies and operations and how digitization capability contributes to cyber resilience. This research will also examine how companies manage investments in cybersecurity, particularly in situations of resource limitations [22].

The research framework is designed to depict the unique digitization capability that supports the formation of cyber resilience and highlight the stages where this capability is most valuable. Thus, these research questions will play a role in exploring the concepts of capability and resilience in the business environment. The research will also explore the potential application of these concepts to address the modern challenges faced by the business world today.

Moreover, this research will identify the role of digitization capability in creating long-term competitive advantages through corporate innovation. This could encompass the development of new products and services that meet customer needs, increased operational efficiency through process automation and integration, as well as enhanced competitiveness through access to broader information and resources.

2. Enabling the Evolutionary Approach in Cybersecurity

Applying a mindset of capability development and preventive protection mechanisms is a fundamental component of the evolutionary approach to cybersecurity [23,24]. This involves transitioning from conventional static security measures to adaptive defense tactics against cyber threats [25]. Through this evolutionary approach, organizations can better adapt to new hazards and establish a stronger security posture by applying evolutionary principles [26].

The evolutionary approach can be used to prevent cyber attacks through a methodological approach involving an evolutionary model. This model depicts how modern cyber–physical systems can counter attacks and evolve, drawing from the experiences of past security incidents. Thus, the evolutionary approach to cybersecurity allows organizations to continually evolve and adapt to new threats, thereby enhancing their resilience against cyber attacks. These efforts encompass developing the ability to anticipate threats, prepare responses to attacks, and swiftly recover operations following incidents.

Furthermore, the evolutionary approach enables organizations to continuously enhance their proactive cybersecurity capabilities. This includes developing security training programs for employees, elevating security awareness throughout the organization, and fostering a strong security culture. Therefore, the evolutionary approach not only aids organizations in responding to cyber attacks but also helps prevent their occurrence.

Moreover, the evolutionary approach allows organizations to collaborate with partners and stakeholders in confronting cyber threats. This involves exchanging information about ongoing threats, successful mitigation strategies, and the latest developments in the field of

cybersecurity. By working together, organizations can collectively identify, analyze, and address threats more effectively.

Overall, the evolutionary approach to cybersecurity provides a comprehensive and flexible framework with which to assist organizations in facing challenges in the current digital era. By applying a mindset of capability development and preventive protection mechanisms, organizations can enhance their resilience against cyber attacks and be prepared to face challenges in the future.

In Figure 1, we present a cybersecurity approach centered around the concept of the resilience paradigm in the digital era. This approach involves several steps:

1. Explore Digital Skills:

Begin by identifying the digital skills required to address cybersecurity threats. Gather information about technical capabilities, transparent processes, and interconnected human factors to establish robust cybersecurity.

2. Analyze Threats and Risks:

Analyze various types of threats that may emerge in the cyber environment, including malware, phishing attacks, DDoS attacks, and other sophisticated threats. Assess the potential risks and impacts of these threats on organizational operations and data security.

3. Develop Threat Response:

Develop a threat response plan encompassing protection, detection, and response measures. Design strategies to rapidly and efficiently counter attacks and recover systems after an incident.

4. Integrate Security and Resilience:

Integrate the concepts of cybersecurity and resilience into the organizational strategy. Create a framework that combines technological aspects, processes, and human factors to achieve resilience against attacks and adaptability.

5. Enhance Readiness and Flexibility:

Build readiness and flexibility to face cybersecurity threats. Design tested incident response plans and possess the capability to swiftly recover systems and data. Adapt to new threats through an understanding of previous attacks.

6. Promote Participation and Collaboration:

Encourage active participation and collaboration from various stakeholders in the cybersecurity ecosystem. Provide financial and non-financial incentives to vendors, business partners, end-users, and other organizations to participate in security and resilience initiatives.

This approach is grounded in a holistic understanding of cybersecurity, where technology, processes, and human factors integrate to create resilience against threats [27,28]. By focusing on the integration of security and resilience and promoting collaboration, organizations can enhance their capabilities to face evolving cybersecurity threats. Evolving methods are facilitated by crucial components such as capability monitoring and threat intelligence. Organizations require reliable solutions to continuously monitor user behavior, system logs, and network activities [29]. By collecting and evaluating relevant data, organizations can learn about new threats, vulnerabilities, and attack trends [17]. This knowledge forms the foundation for proactive decision-making and the implementation of flexible defenses [30].

In Table 2, there is a correlation between cyber resilience and capabilities based on the cybersecurity approach focused on the concept of the resilience paradigm in the digital era. Adaptive defense mechanisms are built on real-time threat data, system behavior, and risk assessment [31,32]. This method allows for dynamic modifications to security rules and response tactics. The evolutionary perspective is crucial; a report by MITRE Corporation found that dynamic cybersecurity methods can increase the detection time of cyber attacks by up to 95%. These data demonstrate that dynamic cybersecurity methods are a more effective way to protect organizations from cyber attacks. This approach enables

organizations to dynamically modify security rules and response tactics based on real-time threat data, system behavior, and risk assessment [33]. This makes it difficult for attackers to breach the organization's security systems. Organizations can stay one step ahead of cyber attackers by continually adapting their defenses to the changing threat landscape. Real-time threat detection and response require the use of technologies such as machine learning, artificial intelligence, and behavior-based analytics [14]. A report by Verizon's Data Breach Investigations Report found that 75% of cyber attacks exploit known vulnerabilities. These data indicate that organizations that do not continuously modify their protection according to the changing threat landscape are more vulnerable to cyber attacks. Therefore, it is important for organizations to implement a comprehensive cybersecurity strategy that includes the use of technologies such as machine learning, artificial intelligence, and behavior-based analytics.

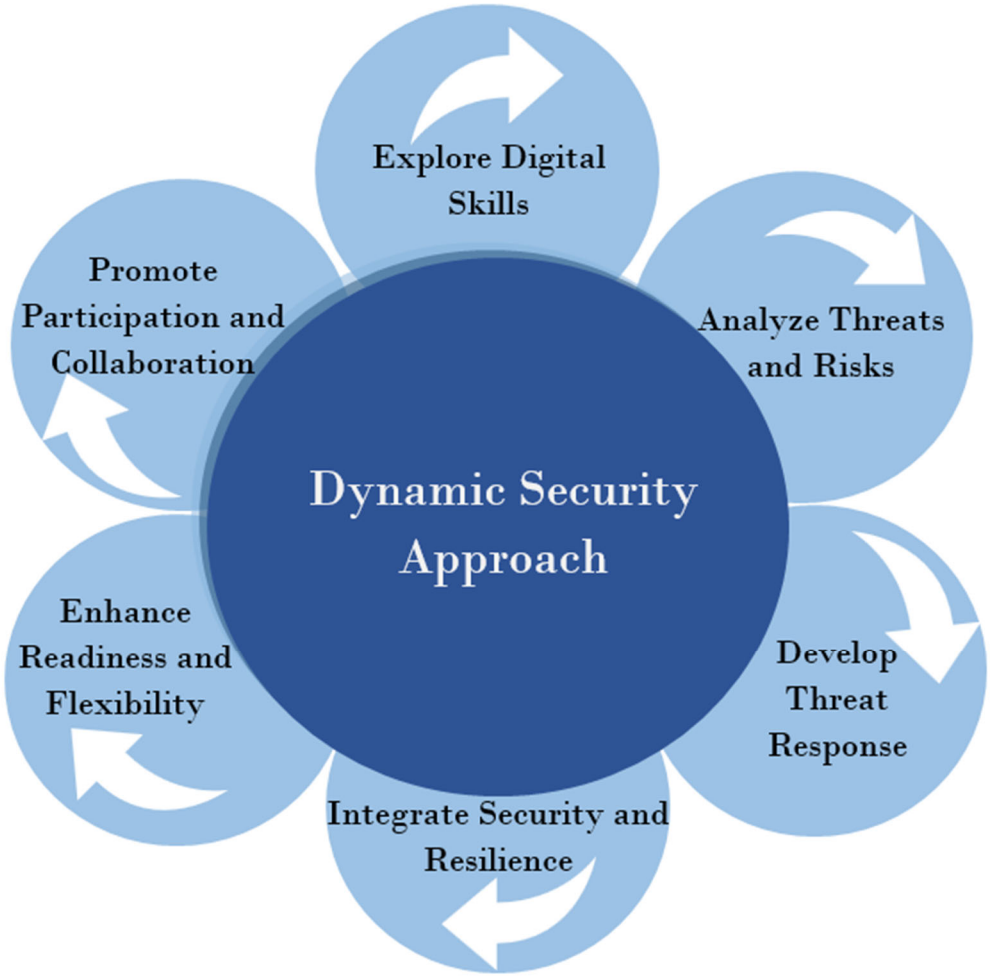

Figure 1. Dynamic security approach.

In the cybersecurity industry, the evolutionary method also promotes cooperative information sharing. Threat information, best practices, and lessons learned should be actively shared among organizations, government agencies, and industry stakeholders [34,35]. This collaborative effort fosters a cooperative defense ecosystem where stakeholders work together to identify and counter new threats. The community can effectively defend against sophisticated cyber attacks that may target multiple entities by combining resources and knowledge [36]. There are various benefits to allowing the evolutionary approach in cybersecurity, particularly making the identification and evasion of cyber attacks easier. Organizations can detect potential threats early on by continuously monitoring and using threat intelligence, enabling quick actions to mitigate risks and prevent successful attacks.

According to Verizon's Data Breach Investigations Report, 82% of data breaches involve insecure sharing of information. According to McAfee, 60% of cyber attacks start with human error exploitation. According to Gartner, organizations that share cybersecurity information can reduce the risk of cyber attacks by 50%.

Table 2. Interconnection between cyber resilience and capabilities.

No	Cyber Resilience	Capabilities	Interconnection between Cyber Resilience and Capabilities
1.	Explore Digital Skills	Identifying the digital capabilities required to address cybersecurity threats. Gathering information about technical capabilities, transparent processes, and interrelated human factors to create robust cybersecurity.	By identifying the required digital capabilities and gathering information about technical skills, transparent processes, and interconnected human factors, organizations can establish robust cybersecurity.
2.	Analyze Threats and Risks	Analyzing various types of threats that may emerge in the cyber environment, including malware, phishing attacks, DDoS attacks, and other sophisticated attacks. Assessing the potential risks and impacts of these threats on organizational operations and data security.	By analyzing various types of threats that may emerge in the cyber environment and assessing the potential risks and impacts of these threats on organizational operations and data security, organizations can develop strategies to respond to attacks quickly and efficiently.
3.	Develop Threat Response	Developing a response plan to threats that includes protection, detection, and response steps. Designing strategies to address attacks swiftly and efficiently, as well as restoring systems after an attack has occurred.	By developing a response plan to threats that encompasses protection, detection, and response steps, as well as designing strategies to address attacks swiftly and efficiently and to restore systems after an attack has occurred, organizations can enhance their resilience to cyber attacks.
4.	Integrate Security and Resilience	Integrating the concepts of cybersecurity and resilience into the organization's strategy. Creating a framework that combines technological aspects, processes, and human factors to achieve resilience against attacks and the ability to adapt.	By integrating the concepts of cybersecurity and resilience into the organization's strategy and creating a framework that combines technological aspects, processes, and human factors to achieve resilience against attacks and the ability to adapt, organizations can enhance their resilience against cyberattacks and improve their capacity to adapt to environmental changes.
5.	Enhance Readiness and Flexibility	Flexibility building preparedness and flexibility in facing cybersecurity attacks. Designing well-tested incident response plans and possessing the capability to swiftly restore systems and data. Adapting to new threats through an understanding of previous attack patterns.	By building preparedness and flexibility in facing cybersecurity attacks, as well as designing well-tested incident response plans and possessing the capability to swiftly restore systems and data, while also adapting to new threats through an understanding of previous attack patterns, organizations can enhance their resilience against cyberattacks and improve their ability to adapt to environmental changes.
6.	Promote Participation and Collaboration	Encouraging active participation and collaboration from various stakeholders within the cybersecurity ecosystem. Providing financial and non-financial incentives to vendors, business partners, end-users, and other organizations to participate in security and resilience initiatives.	By encouraging active participation and collaboration from various stakeholders within the cybersecurity ecosystem, and providing financial and non-financial incentives to vendors, business partners, end-users, and other organizations to participate in security and resilience initiatives, organizations can enhance their resilience to cyber attacks and improve their ability to adapt to environmental changes.

The evolutionary strategy also enhances incident response capacity [14]. Organizations can dynamically adjust their security posture in response to ever-changing threats through adaptive defense mechanisms. Cyber attacks may have a smaller impact if incident response time, containment actions, and overall incident management improve. The evolutionary strategy enhances overall business resilience to cyber attacks. Organizations are better prepared to face and recover from cyber events by continuously implementing and improving security measures [37]. Due to this resilience, companies experience less downtime, smaller financial losses, and maintain their reputation. Organizations must adopt the evolutionary approach to cybersecurity if they want to successfully combat the

rapidly evolving world of online threats. They can enhance detection, incident response, and overall resilience by employing continuous monitoring, adaptive defense systems, and collaborative information sharing [38]. Organizations that embrace the evolutionary approach are prepared to face new challenges and maintain a strong security position against rapidly emerging cyber threats.

3. Cyber Resilience Framework

A report by PwC found that 67% of companies reported experiencing at least one cyber attack in the last 12 months. These data indicate that cyber threats are becoming increasingly serious, and companies need to do more to protect themselves from attacks [38]. Research projects conducted in recent years have helped companies develop frameworks to build resilience against cyber threats. This framework emphasizes goals such as anticipating, defending, recovering, and adapting to reduce the effects of actual or anticipated cyber threats and adapt to changes in mission and business operations [39,40]. The framework provides a step-by-step guide that companies can follow to build resilience against cyber threats [41]. In addition to following the framework, companies also need to enhance cyber threat resilience by investing in cybersecurity technology, educating employees about cybersecurity, having contingency plans for cyber attacks, and conducting regular cybersecurity monitoring [42]. By doing so, companies can enhance their resilience against cyber threats and protect their assets from attacks.

Strategic and tactical resilience models must be created to fully address system risks [43]. In determining the level of vulnerability in the digitalization capability framework, these models consider the vulnerability and reliability levels of hardware and software resources, as well as the functions of physical proximity and networking [44,45]. Creating a robust matrix framework for resilience indicators based on a four-stage lifecycle model: planning/preparation, absorption, recovery, and adaptation. This matrix combines these stages with the doctrinal domains of physical, informational, cognitive, and social aspects of network-centric operations. By combining quantitative and qualitative measurements, the obtained resilience metrics offer a comprehensive evaluation of cybersecurity resilience.

As cyber threats evolve, a risk-based framework has been created that goes beyond conventional risk assessment techniques [46]. This paradigm demonstrates how businesses can build systems that are resilient to changing risks, highlighting the importance of understanding the environment, learning new things, and acquiring specific capabilities to address known and unknown risks.

Jensen and colleagues outlined steps for developing maritime industry cybersecurity resilience, including communication campaigns, consumer awareness, and providing incentives to businesses through "cyber premiums" in insurance plans for adhering to voluntary norms [47]. For a comprehensive examination of cybersecurity, Mase and his team created the Cyber–Physical Security System (CPSS) architecture, encompassing factors such as information security, control, physical security, and recovery plans [48–51]. On the other hand, Annarelli and collaborators developed a resilience management framework and a context-based management framework that guides companies in implementing appropriate steps and investments to enhance cybersecurity resilience.

For successful cybersecurity resilience, they emphasize knowledge management prior to events, security, speed, capacity, and flexibility. It is recommended to adopt an ambidextrous approach in cybersecurity to integrate digitalization capabilities into resilience strategies by integrating balanced scorecards and the multistage 7Ps stage gate model (Patient, Persistent, Persevering, Proactive, Predictive, Preventive, and Preemptive) [52–54]. Despite researchers overcoming the contributions of cyber–physical systems to sociotechnical system resilience, cybersecurity resilience assessment is still in its early stages, and limitations related to comprehensive analysis of the relationship between cybersecurity resilience and digitalization capabilities need to be addressed through further research

to explore potential supporting data and its implications on resilience growth within the digitalization capability framework [55].

In the face of evolving cyber threats, organizations must continuously improve their abilities to manage risks and respond to attacks. This can be achieved through the development of strategic and tactical resilience models that consider the vulnerability and reliability levels of hardware and software resources, as well as physical proximity and networking functions. By creating a robust matrix framework based on a four-stage lifecycle model—planning/preparation, absorption, recovery, and adaptation—organizations can comprehensively evaluate their cybersecurity resilience.

Furthermore, collaboration among organizations, government agencies, and industry stakeholders in sharing threat information, best practices, and lessons learned is crucial in enhancing cybersecurity resilience. Through collaboration, the community can effectively defend against sophisticated cyber attacks that may target multiple entities by combining resources and knowledge.

Thus, collective efforts from all parties involved are essential in comprehensively enhancing cybersecurity resilience. Through close collaboration between organizations, government agencies, and industry stakeholders, as well as the development of strategic and tactical resilience models that consider various aspects of system risks, organizations can build systems that are resilient against rapidly evolving cyber threats. This will help maintain the security of systems and data, as well as protect organizational assets from attacks.

To develop an effective cybersecurity approach, the following stages form the foundation for understanding and implementing the initial cyber security paradigms:

1. Patient reflects a patient attitude in facing cyber threats and risks. Organizations must be capable of observing and understanding the situation patiently before taking action.
2. Persistent refers to consistency in securing systems and data. Cybersecurity must remain an ongoing priority and should not be neglected over time.
3. Persevering signifies that organizations must be resilient in confronting cybersecurity challenges. They need to remain strong in keeping their systems protected even when faced with diverse threats.
4. Proactive emphasizes the importance of preventative measures before threats occur. Organizations should have strategies and tools to identify potential risks before they evolve into actual threats.
5. Predictive emphasizes organizations using data and analysis to predict potential future cybersecurity threat trends. This aids in better planning and response.
6. Preventive involves implementing preventative steps based on predictions and analysis. This involves policy implementation, security tools, and practices designed to prevent threats.
7. Preemptive represents proactive measures taken to address threats before they can disrupt systems. This includes swift responses and more offensive tactics in confronting imminent threats.

By understanding and implementing these stages, organizations can build an effective cybersecurity approach to safeguard their systems and data from evolving cyber threats. Figure 2 visually illustrates how the stages in the multistage 7Ps model are related to the initial cyber security paradigms concepts. Each stage represents a different aspect of the evolution approach in cybersecurity.

Researchers have taken significant steps to address the impact of system resilience. However, it is acknowledged that the assessment of cybersecurity resilience is still in its early exploration stage. In this context, the role of digitalization capabilities in cybersecurity resilience has not been fully revealed through existing studies [56,57]. The close connection between digitalization capabilities and cybersecurity resilience necessitates a more comprehensive research approach. Given this condition, it is imperative to delve deeper into the relationship between digitalization capabilities and cybersecurity resilience through further

in-depth research. The supportive data gathered from such research is expected to provide clearer insights into how the development of digitalization capabilities can contribute to improved cybersecurity resilience [58]. The implications of these findings are expected to offer valuable guidance in enhancing cybersecurity resilience in the ever-evolving digital era.

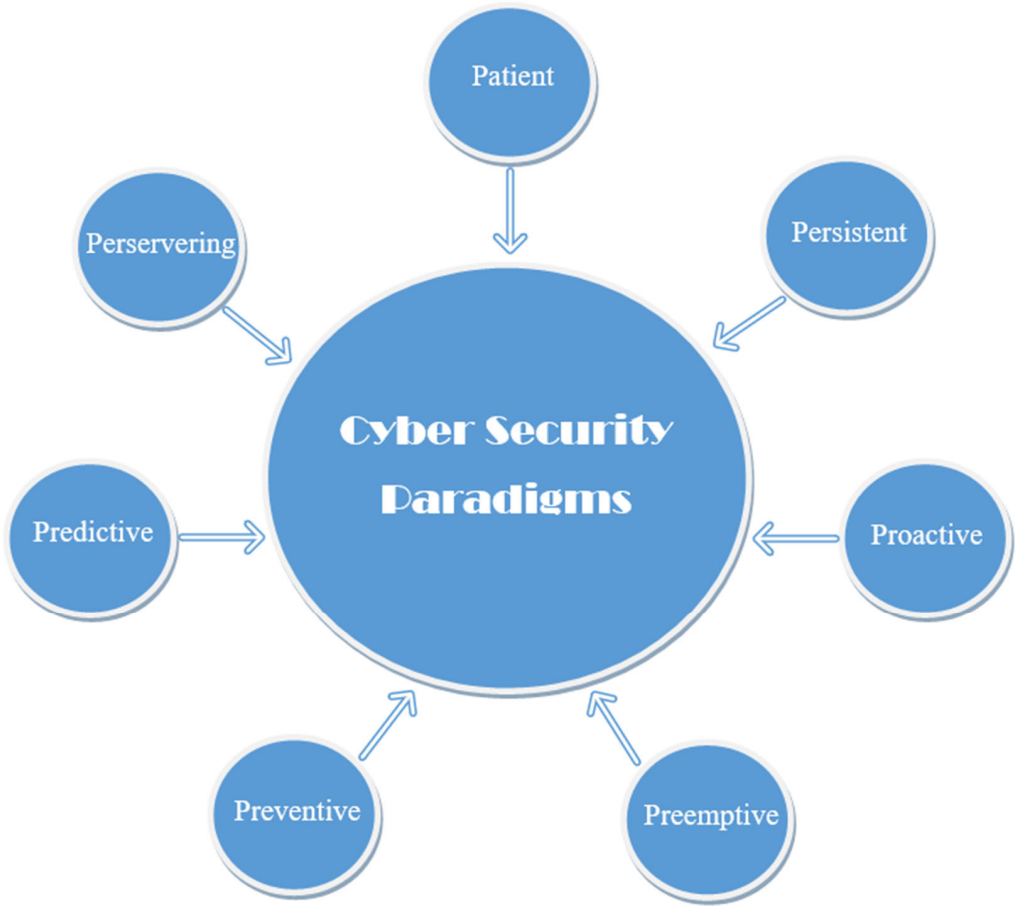

Figure 2. Evolution of cyber security paradigms: stage gate 7Ps multistage model.

Amid the increasing threats in the digital realm, an innovative holistic approach is needed to address the existing challenges. Hence, a new paradigm is proposed to comprehensively enhance cybersecurity resilience. This paradigm embraces three main concepts—cyber shield, cyber space, and cyber resilience—which are integrated into a harmonious unity. Cyber shield aims to prevent attacks early, cyber space focuses on the capacity to withstand and adapt to attacks, while cyber resilience emphasizes the ability to recover and restore after disruptions. Within this paradigm, each concept plays a key role in securing digital systems against various threats. In a world where cyber attacks are becoming more complex and widespread, the integration of these three concepts is expected to provide a solid framework for effectively responding to security challenges in the digital era [59,60]. Thus, this paradigm serves not only as a theoretical foundation but also as a practical action guide in addressing the evolving threats and risks in the current digital environment.

First, we present the design for a cyber defense concept called "Cyber Shield". This idea refers to a robust cybersecurity strategy to defend systems and networks from attacks. Tight security procedures, advanced technology implementation for detection, prevention, and response to attacks, as well as proactive monitoring of new threats, are all part of the Cyber Shield. The primary protector used to shield companies from cyber threats is called a cybersecurity guard.

Second, the concept of cyber resistance, which we call "Cyber Space", represents efforts to enhance resistance against successful attacks that bypass frontline defenses. To reduce the impact of attacks and ensure operational continuity, Cyber Space employs strategies including early detection, rapid response, effective recovery, and the use of adaptive technology. The concept of "Cyber Space" refers to the tactical area where companies can reinforce their security measures and protect system integrity when facing cyber attacks [61].

Third, we present the concept of Cyber Resilience, which we label as "Cyber Sword". This concept refers to an organization's capacity to adapt and resist cyber attacks. Cyber Sword involves proactive and defensive tactics that utilize a deep understanding of cyber threats, employing offensive strategies such as digital forensic analysis, developing new security capabilities, and implementing dynamic defense measures. Cyber Sword represents an organization's ability to confront cyber attacks with courage and resilience.

Organizations can objectively analyze their security measures, identify areas for improvement, and recognize strengths by aligning this paradigm with its related metrics [62]. With methodical techniques, companies can move beyond vague assessments and measure the actual effectiveness of their security initiatives [63].

Thus, a comprehensive approach to cybersecurity involves a combination of proactive and reactive defense strategies and the ability to adapt to evolving threats. Through the harmonious implementation of the Cyber Shield, Cyber Space, and Cyber Sword concepts, organizations can enhance their resilience against cyber attacks and protect their assets.

Table 3 below provides a mapping of the stage gate 7Ps multistage indicators to the indicators of Security as a Shield, Security as a Space, and Security as a Sword. This table demonstrates how these indicators can be aligned with commonly used cybersecurity frameworks or standards, such as the NIST Cybersecurity Framework and ISO 27001 Information Security Management System (ISMS) Standard [64]. The table also provides descriptions and implications of each indicator, aiding organizations in understanding how these indicators can be used to enhance overall cybersecurity resilience. This mapping is just one way to organize and comprehend these indicators, and specific details may vary depending on organizational context and needs.

Table 3. Cyber security paradigms indicator mapping.

No	7Ps Multistage	Indicator	Framework or Standard	Description	Implication
1.	Patient	Awareness	NIST Cybersecurity Framework	The ability to remain calm and composed in the face of adversity and to continue working towards a goal despite setbacks.	A patient approach to security can help organizations to build a strong foundation of awareness and understanding, which can improve their overall resilience.
2.	Persistent	Assurance	NIST Cybersecurity Framework	The ability to continue working towards a goal despite obstacles or setbacks and to maintain focus and determination over time.	A persistent approach to security can help organizations to build robust systems and processes that provide assurance of their resilience.
3.	Persevering	Protection	NIST Cybersecurity Framework	The ability to continue working towards a goal despite significant challenges or adversity and to maintain focus and determination, even in the face of failure.	A persevering approach to security can help organizations to build strong defenses that protect against threats and improve their overall resilience.
4.	Proactive	Management	NIST Cybersecurity Framework	The ability to anticipate potential challenges or threats and to take action to prevent or mitigate them before they occur.	A proactive approach to security can help organizations to manage risks effectively and improve their overall resilience.

Table 3. *Cont.*

No	7Ps Multistage	Indicator	Framework or Standard	Description	Implication
5.	Predictive	Principles	ISO 27001 Information Security Management System (ISMS) Standard	The ability to use data and analysis to anticipate future trends or events and to make informed decisions based on this information.	A predictive approach to security can help organizations to develop sound principles that guide their decision-making and improve their overall resilience.
6.	Preventive	Policy	ISO 27001 Information Security Management System (ISMS) Standard	The ability to take action to prevent potential challenges or threats from occurring, rather than simply reacting to them after they have happened.	A preventive approach to security can help organizations to develop effective policies that reduce their exposure to risk and improve their overall resilience.
7.	Preemptive	Capabilities	ISO 27001 Information Security Management System (ISMS) Standard	The ability to take decisive action to prevent or mitigate potential challenges or threats before they occur, even if this requires making difficult decisions or taking bold risks.	A preemptive approach to security can help organizations to build strong capabilities that enable them to respond effectively to emerging threats and improve their overall resilience.
8.	Patient	Culture	ISO 27001 Information Security Management System (ISMS) Standard	The ability to remain calm and composed in the face of adversity and to continue working towards a goal despite setbacks. This includes fostering a culture of security awareness within the organization.	A patient approach can help organizations develop a strong culture of security awareness that supports their overall resilience.
9.	Persistent	Readiness	NIST Cybersecurity Framework	The ability to continue working towards a goal despite obstacles or setbacks and maintaining focus and determination over time to be ready for potential challenges or threats.	A persistent approach can help organizations develop robust systems and processes that support their readiness for potential challenges or threats.
10.	Persevering	Recovery	NIST Cybersecurity Framework	The ability to continue working towards a goal despite significant challenges or adversity, maintaining focus and determination even in the face of failure in order recover from incidents.	A persevering approach can help organizations develop strong capabilities for recovering from incidents that impact their security.

4. Cyber Resilience Paradigm in the Digital Age

In Figure 3, we employed a series of research procedures to examine the relationship between digitalization capabilities and cybersecurity resilience. We began with a literature review involving previously researched digitalization capabilities. Subsequently, we conducted a replication search within the online Scopus database using specific search terms. Scopus was chosen as the data source due to its solid reputation for works published after 1995, as well as its broad subject coverage and journal range. We applied the recommendations and standards previously mentioned in this study to establish inclusion and exclusion criteria in the selection of relevant literature. The proposed research design framework was employed, as outlined in the publication "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity".

The research procedures we undertook, the methodology we applied, the results of the literature review, and the conceptual framework we devised are elaborated in-depth in this study. This research aims to provide a clearer understanding of the relationship between digitalization capabilities and cybersecurity resilience. We believe that our research can furnish valuable insights in addressing cybersecurity risks and better planning for the future of cybersecurity.

Figure 3. Research procedure resilience paradigm.

5. Connecting the Dots beyond Resilience

This debate focuses on the significance of adopting a broader perspective when developing cybersecurity resilience. Understanding the intricate and interconnected interactions between these components is as crucial as comprehending the fundamental concepts and essential elements of cybersecurity resilience. Integrating these ideas comprehensively enables companies to address cybersecurity issues swiftly and effectively.

One approach to gaining a broader perspective is by considering all aspects of cybersecurity resilience. This encompasses technical aspects such as hardware and software security, as well as non-technical aspects such as security culture and employee awareness. It is essential to grasp how these aspects interrelate and how they contribute to the overall resilience of an organization. Another way to broaden the view is by considering the entire lifecycle of cybersecurity resilience. This includes prevention, detection, and response. Strong strategies are vital for all three stages. Prevention strategies should be designed to thwart attacks from occurring in the first place. Detection strategies should be crafted to swiftly identify and respond to attacks. Response strategies should be designed to recover organizations from attacks and mitigate the impacts of said attacks.

Table 4 illustrates how the indicators of Security as a Shield, Security as a Space, and Security as a Sword can be mapped to industry and organizational requirements. This table also provides implications of each indicator for industries and organizations, along with aspects and parameters related to each indicator. Therefore, this table can aid industries and organizations in comprehending how these indicators can be utilized to enhance overall cybersecurity resilience.

Table 4. Mapping cyber security paradigms indicators for industry and organizations.

No	Indicator	Industry/Organization Implication	Aspect	Parameters
1.	Awareness	Industries and organizations need to be aware of the potential threats and risks they face to develop effective strategies for managing them.	Threat Landscape	Understanding the threat landscape, identifying vulnerabilities, staying up to date with the latest trends and developments in security.
2.	Assurance	Industries and organizations need to have confidence in their ability to manage risks and withstand disruptions.	Preparedness	Having robust systems and processes in place that provide assurance of resilience, regularly testing and evaluating preparedness.
3.	Protection	Industries and organizations need to have strong defenses in place to protect against threats.	Defense Measures	Implementing appropriate security measures such as firewalls, intrusion detection systems, access controls, regularly monitoring for suspicious activity.
4.	Management	Industries and organizations need to be proactive in managing risks and responding to potential disruptions.	Risk Management	Having effective incident response plans in place, regularly reviewing, and updating security policies and procedures.
5.	Principles	Industries and organizations need to have a clear set of principles that guide their decision-making when it comes to security.	Risk Management Framework	Having a well-defined risk management framework, clear guidelines for how risks should be assessed and addressed.
6.	Policy	Industries and organizations need to have effective policies in place that support their overall security posture.	Data Handling Rules	Having clear rules and guidelines for how data should be handled, policies for managing access to sensitive information.
7.	Capabilities	Industries and organizations need to have the necessary capabilities in place to respond effectively to emerging threats.	Response Capabilities	Having the right tools, technologies, expertise available, regularly investing in training and development to build capabilities over time.
8.	Culture	Industries and organizations need to foster a culture of security awareness within their workforce.	Security Awareness Culture	Providing regular training and education on security best practices, encouraging employees to take an active role in protecting the organization's assets.
9.	Readiness	Industries and organizations need to be ready to respond quickly and effectively to potential disruptions or incidents.	Incident Response	Having effective incident response plans in place, regularly testing readiness through exercises or simulations.
10.	Recovery	Industries and organizations need to have effective plans in place for recovering from incidents that impact their security.	Business Continuity	Having backup systems in place, clear procedures for restoring operations after an incident has occurred.

By adopting a broader perspective, companies can develop stronger cybersecurity resilience. Enhanced cybersecurity resilience will aid companies in safeguarding their assets and data from cyberattacks, allowing them to continue operations even in the face of such attacks. Here are specific examples of how companies can take a broader view to enhance their cybersecurity resilience: Companies can invest in cybersecurity technologies that help them prevent, detect, and respond to cyberattacks [65]. Companies can educate their employees about cybersecurity and how to protect themselves from cyber threats.

Companies can formulate contingency plans for cyberattacks to ensure the continuity of their operations even during an attack. By taking these steps, companies can bolster their cybersecurity resilience and shield themselves from cyber threats.

Furthermore, companies can collaborate with others to enhance their cybersecurity resilience. For instance, companies can partner with cybersecurity service providers to ensure they have the best available protection. They can also engage with industry organizations or working groups to share information about cyber threats and best practices for defense. Through collaboration, companies can leverage expertise and experiences from various sources to enhance their cybersecurity resilience. Additionally, companies must ensure they comply with all relevant regulations and standards for cybersecurity, such as the ISO 27001 standard for information security management. By taking these measures, companies can cultivate stronger cybersecurity resilience and fortify themselves against cyberattacks.

5.1. Cyber Resilience Factors Model

Cybersecurity resilience is an organization's ability to identify, protect against, detect, respond to, and recover from cyberattacks. This concept involves coordinated efforts encompassing organizational, technological, and human factors [66,67]. The appropriate use of policies, processes, and strategies to maintain continuous operations and safeguard data and infrastructure from cyber threats is essential for achieving cybersecurity resilience. In Figure 4, factors contributing to cybersecurity resilience are depicted:

- Security culture: Cybersecurity must be ingrained in the organizational culture. Every employee should be aware of the significance of cybersecurity and play a role in safeguarding the organization against cyberattacks.
- Technology: Organizations should invest in cybersecurity technologies that help them prevent, detect, and respond to cyberattacks.
- Processes: Organizations should have well-documented and routinely tested cybersecurity processes. These processes should encompass steps to identify, protect against, detect, respond to, and recover from cyberattacks.
- Strategy: Organizations should possess a comprehensive cybersecurity strategy. This strategy should encompass goals, objectives, and actions to achieve cybersecurity resilience.
- People: Human elements are often overlooked in cybersecurity discussions. However, people are frequently the weakest link in the security chain. Organizations need to ensure that their employees are aware of risks and know how to protect themselves and the organization.

Here are some additional factors that can contribute to cybersecurity resilience:

- Visibility: Organizations need visibility into their IT environment to promptly identify and respond to threats.
- Communication: Organizations need effective communication channels to quickly share information about threats and incidents.
- Exercises: Organizations should regularly conduct security exercises to test their readiness to respond to attacks.
- Continuous improvement: Organizations should consistently enhance their security posture by regularly reviewing their security controls and processes.

By considering these factors, organizations can enhance their resilience against cyberattacks. Stronger cybersecurity resilience will help organizations protect their assets and data from cyberattacks and enable them to continue operations even in the face of such threats.

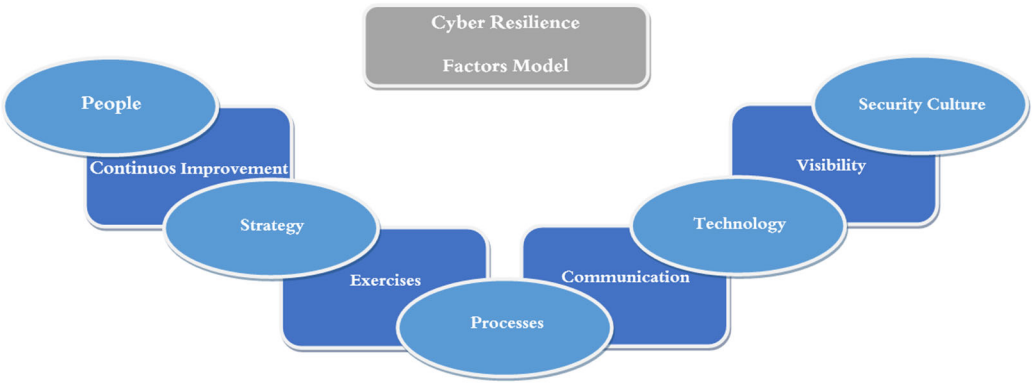

Figure 4. Cyber resilience factors model.

5.2. Key Components of Cyber Resilience

The fundamental goal of cybersecurity resilience is to identify the crucial, interconnected, and mutually beneficial elements of cybersecurity resilience. To achieve successful cybersecurity resilience, it is essential to consider technological security, transparent rules, and processes, as well as human factors. In Figure 5, organizations can establish effective and swift defense against cyberattacks by combining these three elements.

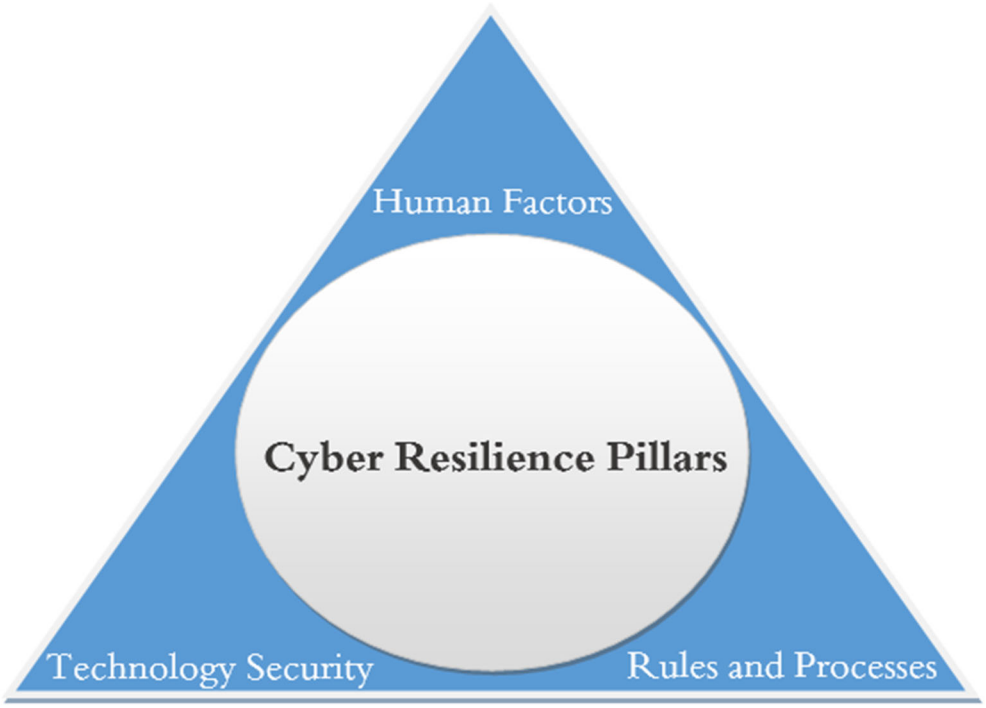

Figure 5. Cyber resilience pillars.

- Technology security: Organizations need to invest in appropriate security technologies to protect their systems and data. This includes firewalls, intrusion detection systems, and antivirus software. Organizations also need to implement best security practices, such as using strong passwords and enabling multi-factor authentication.
- Rules and processes: Organizations need to have clear and transparent security rules and processes. This will help employees understand their responsibilities for security and how to report security incidents. Organizations also need well-defined recovery processes to respond to cyberattacks.
- Human factors: Humans often represent the weakest link in the security chain. Organizations need to ensure that their employees are aware of security risks and know

how to protect themselves and the organization. Organizations should also provide regular security training to their employees.

By combining these three elements, organizations can establish effective and rapid defense against cyberattacks. Cybersecurity resilience is an ongoing process, and organizations need to continuously enhance their security posture in response to evolving threats.

5.3. Understanding Cyber Resilience Threats and Risks

A deep understanding of the risks and threats in the cyber environment is of utmost importance. Threats such as malware, phishing attacks, distributed denial of service (DDoS), and advanced persistent threats (APTs) need to be thoroughly comprehended. Additionally, perils such as data loss, identity theft, financial losses, and reputational damage also require vigilance [68]. Malware encompasses software that damages or steals data, including viruses, worms, Trojans, and ransomware. Meanwhile, phishing attacks involve deceptive attempts, disguising themselves as trustworthy sources to acquire personal information. DDoS is a flooding attack that disrupts services, and advanced persistent threats (APTs) are designed by nations or state actors to steal sensitive information [69]. Furthermore, hazards can also manifest as critical data loss, identity theft, financial losses, and reputational harm. To confront these threats, it is crucial to conduct in-depth studies, identify vulnerabilities, and mitigate current risks [70]. Some steps that can be taken include updating software, using strong and unique passwords, enabling multi-factor authentication, exercising caution when opening emails and links, and safeguarding personal information. Designing a responsive plan for cyberattacks is also imperative. Through these measures, organizations can significantly diminish the risk of cyberattacks and shield themselves from various potential perils.

5.4. The Importance of Readiness and Adaptability in Cyber Resilience

Organizations must possess a well-planned and tested incident response strategy, in addition to implementing preventive measures. We emphasize the crucial importance of swiftly restoring systems and data. Furthermore, flexibility becomes essential in facing emerging threats. Organizations need the ability to adapt their systems and security methods over time, learning from past attacks, identifying new vulnerabilities, and other factors. In Figure 6, the steps that organizations can take to enhance their readiness and agility in facing cyberattacks are outlined:

- Incident Response Plan → have a planned and tested incident response strategy.

The incident response strategy should encompass the actions the organization will take during a cyberattack. These actions should include identifying the attack, isolating impacted systems, restoring systems and data, and conducting an investigation.

- Threat Protection → mitigate against threats.

Organizations need to engage in mitigation efforts against various cyber threats such as malware, phishing attacks, and DDoS attacks. Mitigation can be achieved through implementing various security measures, including using strong passwords, enabling multi-factor authentication, and keeping systems up-to-date.

- System and Data Recovery → have a plan to recover systems and data.

Organizations need to have a comprehensive plan in place for recovering systems and data in the event of a cyberattack. This plan should outline the steps the organization will take to restore systems and data as swiftly as possible.

- Agility and Adaptability → be flexible.

Organizations need to demonstrate flexibility and the ability to adapt their systems and security methods over time. This adaptability is crucial as cyber threats continue to evolve, and organizations must be prepared to respond to new threats.

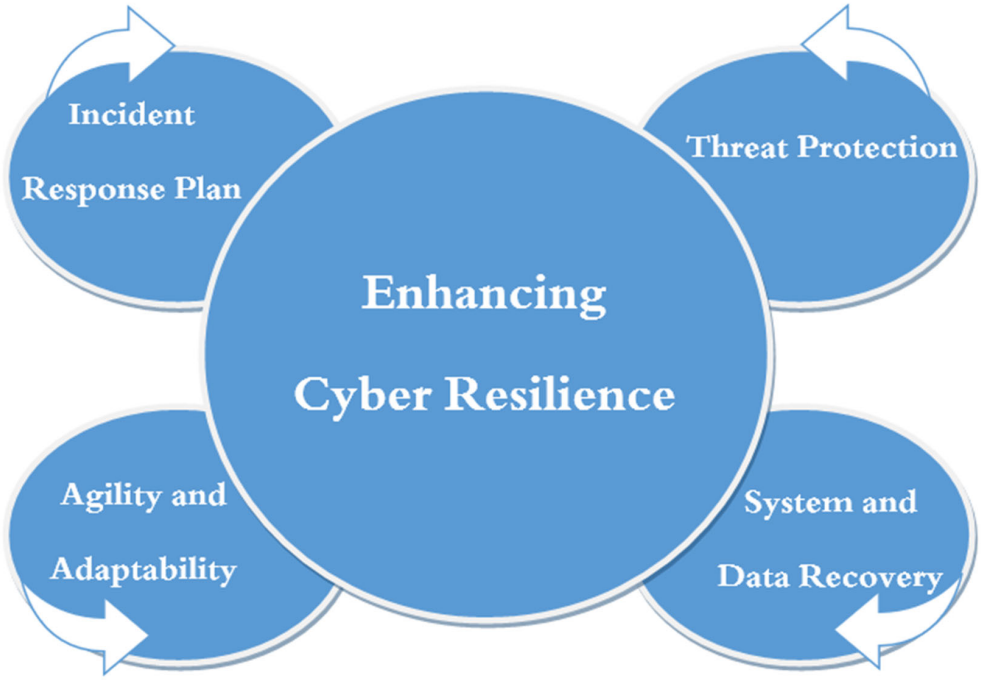

Figure 6. Enhancing cyber resilience.

By implementing these steps, organizations can develop effective defenses against cyberattacks. Cyber resilience is an ongoing process, and organizations need to continuously enhance their security posture as threats evolve.

To bolster cybersecurity, organizations must ensure they possess an effective and tested incident response strategy, alongside implementing appropriate preventive measures. However, cybersecurity is not solely about preventing attacks; it also involves swiftly recovering systems and data post-attack. Therefore, flexibility is of paramount importance in facing emerging threats. Organizations must be capable of adapting their security systems and methods over time, learning from past incidents, identifying new vulnerabilities, and other relevant factors. By undertaking these actions, organizations can enhance their readiness and adaptability in the face of cyberattacks, thereby reducing the risk of such attacks and protecting themselves from potential losses.

Additionally, organizations should collaborate with external entities to enhance their cybersecurity resilience. For instance, they can partner with cybersecurity service providers to ensure they have the best available protection. Organizations can also join industry associations or working groups to share information about cyber threats and best practices for defense. Through collaboration, organizations can leverage expertise and experiences from diverse sources to enhance their cybersecurity resilience.

In conclusion, there are numerous steps organizations can take to enhance their cybersecurity resilience. These steps encompass the development of effective and tested incident response strategies, the implementation of suitable preventive measures, an increase in adaptability to face emerging threats, and collaboration with external entities to boost cybersecurity resilience. By taking these measures, organizations can shield themselves from cyberattacks and continue their operations even in the face of an attack.

6. Incentivizing the Channel: A Key Aspect of Resilience

Organizations need to focus not only on cybersecurity but also on resilience factors to address the increasingly complex and diverse landscape of cyberattacks. Resilience reflects an organization's ability to anticipate, withstand, recover, and adapt to cyber disasters, while cybersecurity aims to protect systems and networks from unauthorized access and attacks.

In Figure 7, an integrated flow from initial planning to subsequent planning is depicted, with a focus on sustaining and continuously enhancing organizational resilience:

1. Resilience Planning: Ensure initial steps where organizations plan their overall approach to resilience. This may involve risk identification, goal setting, and developing a general strategy to address challenges.
2. Plans Implementation: After planning, organizations create concrete plans to address identified risks and challenges. These plans are designed to remain effective in evolving and complex situations.
3. Resilience Activities: Execute the plans through various activities. This step involves implementing actions designed to reduce risk impact and enhance organizational resilience.
4. Capacities: Through a series of activities and actions, organizations build capacities that enable them to respond and readapt to challenging situations.
5. Resilience Measurement: Ensure the effectiveness of resilience plans and activities by measuring performance and the impact of implemented measures.
6. Capability: Display the ability to effectively listen and respond to input, feedback, or signals of change, which is crucial in building adaptive resilience.
7. Innovation: Develop new approaches to tackle evolving challenges. Organizations need to find novel ways to respond to changing environments.
8. Improvements: Grounded in measurements and input, organizations continually refine their plans, activities, and capacities, ensuring their relevance and effectiveness.
9. Resilience Planning (Continuation): This cycle then continues with re-planning based on previous learning and experience, forming a continuous loop.

Figure 7. Resilience enhancement roadmap.

In the digital era, it is crucial for organizations to successfully combat cyber threats and uphold security. The convergence between cybersecurity and resilience is essential [71,72]. Organizations can design comprehensive strategies to protect against evolving cyber threats by integrating both concepts. Offering incentives to relevant channels or stakeholders is a vital element of this integration. This step encourages the cybersecurity ecosystem, business partners, end-users, and other organizations to interact and actively participate. Finan-

cial and non-financial incentives can help enhance awareness, capabilities, and readiness to face cyber risks. Organizations can build strong partnerships within the cybersecurity ecosystem, raise awareness about threats and risks, and support each other in confronting complex challenges. The efficiency of security and resilience initiatives can be elevated through support and active engagement of relevant stakeholders. By fostering this collaboration, organizations can reinforce their understanding and culture of cybersecurity within the organization and its affiliates [73].

Overall, creating robust cybersecurity and resilience necessitates providing incentives to channels [74,75]. Organizations can bolster their ability to tackle increasingly complex cyber threats while maintaining efficient operations and capabilities in a continually changing digital era. Through active engagement, improved collaboration, and the development of a strong security culture, organizations can create a secure and resilient environment against existing and upcoming cyber challenges.

Financial incentives can drive the development of advanced security technologies and innovative resilience solutions. Such financial support can also be used to provide training and skill enhancement to personnel involved in cybersecurity and resilience. For instance, providing financial incentives to cybersecurity teams to develop more advanced analytical tools or conduct attack simulations can encourage an increase in the organization's capabilities to face complex threats. Alongside financial incentives, non-financial incentives also play a significant role. Recognition of individual and team contributions to maintaining security and resilience can enhance motivation and commitment. Acknowledgment of achievements in confronting cyber threats can foster a strong security culture throughout the organization. Furthermore, through appropriate incentives, organizations can establish strong partnerships within the cybersecurity ecosystem. Business partners, vendors, and actively engaged end-users can mutually support one another in facing complex challenges. This collaboration can result in more holistic and effective solutions to address a variety of cyber threats.

Efficiency in security and resilience initiatives can also be enhanced through the support and active involvement of relevant stakeholders. By involving all relevant parties, organizations can ensure that the steps taken align with their needs and expectations. Overall, integrating cybersecurity and resilience and providing appropriate incentives to all stakeholders are critical steps in confronting evolving cyber threats. Only through a comprehensive and collaborative approach can organizations create a secure, resilient, and prepared environment to face the current and future challenges of the ever-changing digital era.

7. Uplifting Resilience toward Cyber Threat: Enhancing the Ability to Mitigate Risks

The cybersecurity resilience framework is a collection of processes, policies, and procedures designed to assist organizations in identifying, preventing, detecting, responding to, and recovering from cyberattacks [76]. This framework involves several aspects, including management considerations, organizational elements, and technology. In Figure 8, a robust cybersecurity resilience framework is depicted, containing the following key elements:

1. Risk Assessment and Management: Conduct a comprehensive evaluation of potential cyber risks and develop risk management strategies to mitigate the impact and likelihood of these risks.
2. Incident Response and Recovery: Formulate a clear incident response plan, outlining the steps to be taken during cyber incident situations, including rapid recovery and operational restoration schemes.
3. Technology and Infrastructure: Utilize secure network design, encryption protocols, access restrictions, and continuous system and infrastructure monitoring as strong cybersecurity measures that must be implemented.
4. Human Variables: Highlight the understanding of cybersecurity and acknowledge that employees play a role that can affect cybersecurity resilience. This is achieved by fostering a culture of understanding and responsibility among workers, promot-

ing cybersecurity training, and ensuring their active participation in maintaining corporate security.

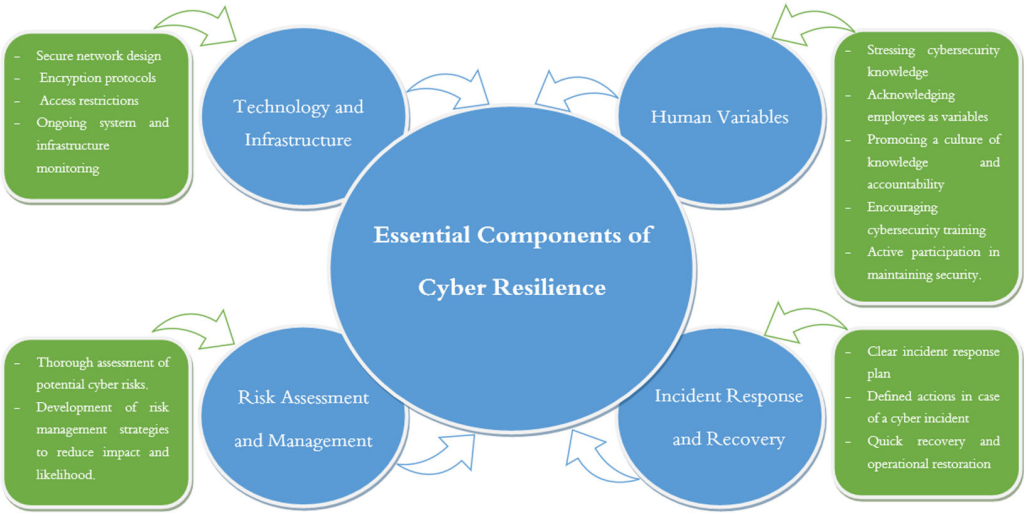

Figure 8. Essential components of cyber resilience.

The success of implementing cybersecurity resilience techniques heavily relies on governance and leadership. Organizational leaders must demonstrate strong commitment to cybersecurity and resilience through fund allocation, formulation of clear policies, and stakeholder direction. To ensure the organization's efforts in building cybersecurity resilience align with regulations and standards, the governance structure should also involve accountability procedures, risk management, and compliance [77,78]. Leadership engagement is key in shaping a culture that prioritizes cybersecurity, encourages collaboration, and supports continuous resilience capability development. Through the integration of cybersecurity and resilience, the development of a comprehensive framework, emphasis on critical aspects, and focus on governance and leadership, organizations can enhance their cybersecurity resilience and achieve sustained security in the face of evolving digital capabilities and cybersecurity threats [57].

This cybersecurity resilience framework brings various benefits:

- Reducing the risk of cyberattacks.
- Enhancing the speed and effectiveness of recovery from cyber incidents.
- Improving operational efficiency.
- Lowering cybersecurity costs.
- Enhancing customer satisfaction.
- Boosting organizational reputation.

By implementing the cybersecurity resilience framework, organizations can elevate their security level and mitigate the risk of cyberattacks.

8. Understanding Capabilities: The Critical Path

By integrating the flows of physical, financial, and informational aspects with supply chain partners, businesses need to build partnership-oriented capabilities within the digital ecosystem. To discover and leverage capabilities within the digital ecosystem, they also need to enhance their digital innovation capabilities. While using information technology as a driver of digital competitiveness, businesses must maximize their own digitization capabilities. Beyond a comprehensive examination of the nature of digitization capabilities, another contribution is investigating the adoption of digitization capabilities by leveraging heterogeneous resources that enable digital solutions while considering various phases of the business process.

The ability to digitize is crucial for work automation and information sharing. The company's digital resources and processes need to be reconfigured. An important capability is the ability to rapidly reconfigure resources, especially concerning digital innovation initiatives [79]. Conceptualizing the capacity of dynamic network empowerment, which, in turn, enables simultaneous processing and management of numerous innovations at a specific time, is based on the idea of digital integration capability. This is closely connected to work that formalizes the significance of scanning the evolution of the digital environment while seeking digital innovation opportunities. This is a critical factor, especially when speaking about improvisation capability, which is explored in the same research. The authors claim that "the flexibility of digital technology allows for a higher level of improvisation than their analog counterparts". Further in-depth research is conducted on this subject and its applicability. "The capacity to spontaneously rebuild existing resources to develop new operational capabilities to deal with urgent, unforeseen, and novel environmental situations" is how improvisation capability is described [80]. The significance of adaptation in the context of digital marketing is also emphasized by this research. Finally, offering advice on how to apply digital technology in the real world, assisting managers and scientists in understanding the potential impact of digital technology on the supply chain [81].

When considering the indicated contributions, the digitization capabilities studied in this research that are involved in the cybersecurity resilience process include the following:

(a) Leveraging heterogeneous resources.
(b) Improvisation capability.
(c) Online information capabilities.
(d) Promoting continuous learning.
(e) Evolution of digital environmental scanning.
(f) Timely resource reconfiguration.

The conceptual framework discussed more deeply in the following section has been updated to encompass these potential digitization capabilities. We aim to analytically demonstrate that each digitization capacity has implications for cybersecurity resilience to contribute theoretically and practically to this research trajectory. We found several interesting connections between digitization capabilities and cybersecurity resilience practices in the proposed managerial cybersecurity resilience framework. The managerial cybersecurity resilience framework is our first choice due to its emphasis on management practices and alignment with ideas about digital capabilities [82,83].

Digital capabilities that support cybersecurity resilience, related cybersecurity resilience strategies, and associated cybersecurity resilience stages are listed in Table 5 below.

(a) Employing Heterogeneous Resources: The ability to utilize various distributed resources to implement digital solutions at different levels and stages of the business process. There is a distinction between digital capabilities for job automation and digital capabilities for information exchange and processing.
(b) Improvisational Capabilities: The capacity to rapidly adapt current resources to create new operational abilities to confront urgent, unforeseen, and novel environmental challenges. This is achieved by effectively leveraging digital IT systems.
(c) Online Informational Capabilities: Through the integration of IT resources and processes, businesses can share strategic and tactical information.
(d) Fostering Continuous Learning: Businesses must promote continuous learning about the unique characteristics of digital technology by developing new roles and cultivating new sets of internal and external capabilities.
(e) Examining the Evolution of the Digital Environment: Companies should scrutinize their digital environment's conditions to identify opportunities and recognize significant changes.
(f) Timely Resource Reconfiguration: The ability to provide enhanced digital business network connectivity to swiftly deliver value to customers.

Table 5. Digitalization capabilities driving cyber resilience.

No	Digitalization Capabilities	Cyber Resilience Practice	Cyber Resilience Phase
1.	Employing Heterogeneous Resources	Prevention	Plan/Prepare
2.	Employing Heterogeneous Resources	Training	Plan/Prepare
3.	Improvisational Capabilities	Update	Adapt
4.	Online Informational Capabilities	Prevention	Plan/Prepare
5.	Online Informational Capabilities	Review	Adapt
6.	Scanning Evolution of Digital Environment	Adaptation to the Context	Adapt
7.	Timely Reconfiguration of Resources	Adaptation to the Context	Adapt
8.	Promoting Continuous Learning	Training	Plan/Prepare
9.	Scanning Evolution of Digital Environment	Context	Adapt
10.	Timely Reconfiguration of Resources	Context	Adapt

In conclusion, there are synergistic opportunities when many digitization capabilities are adopted and developed concurrently. A comprehensive strategy for addressing cybersecurity threats can be provided by incorporating these capabilities into the cybersecurity resilience architecture.

9. Developing a Future-Ready Digital Organization

The operations of organizations have undergone a radical transformation due to digitization, which has also introduced new and challenging cybersecurity issues. To ensure long-term security, we have provided a comprehensive method for developing a cybersecurity resilience framework that incorporates the digitization capabilities explored in this research. We have identified essential digitization capabilities through our research and analysis that align with various phases of cybersecurity resilience. According to our findings, the use of diverse resources is crucial for training and prevention within the scope of cybersecurity resilience. Given variations in information-sharing capabilities and process automation, organizations must employ digital solutions at various points and phases of their business processes. By efficiently utilizing digital IT systems, improvisational capabilities enable companies to respond to urgent and novel environmental events. Integrating online information capabilities is vital for prevention and cybersecurity review procedures. Organizations need to integrate IT resources and procedures to securely share strategic and tactical information. To detect opportunities and understand significant changes in their digital landscape, companies should scan the evolution of the digital environment throughout the adaptation phases [84]. Network activation capabilities provide timely resource reconfiguration, enabling companies to adapt to contexts and accommodate customer-value-driven business innovations.

We have identified the primary strengths influencing cybersecurity resilience in managerial processes based on previously developed ideas. During the planning and preparation phases, prevention and training activities are driven by leveraging diverse resources and promoting continuous learning. The planning, preparation, and adaptation phases each involve related prevention and review techniques driven by online information capabilities. Update procedures, as utilized in the adaptation phase, are driven by improvisational capabilities. The adaptation phase, also driven by digital environmental scanning and rapid resource reconfiguration, encompasses adaptability to context. Future empirical research could build upon these conclusions to validate and further delve into the relationship between digitization capabilities and cybersecurity resilience. We emphasize how crucial it is for scholars and practitioners to focus on how digitization capabilities and cybersecurity

resilience mutually benefit each other. This partnership serves as a critical turning point in mastering corporate digital transformation [85]. Additional digital capabilities contributing to resilience and business strategies could be discovered through further investigation into cybersecurity resilience methods [86,87]. To achieve cybersecurity resilience and succeed in their digital business transformation, companies must understand and harness the complex nature of digitization capabilities.

To achieve long-term security, this research has demonstrated the significance of integrating digitization capabilities into the cybersecurity resilience architecture. Organizations can enhance their capacity to prevent, adapt to, and recover from cyber disasters in the digital era by utilizing tools, technology, and digital practices [88]. The suggested framework and provided recommendations offer useful guidance to companies on how to enhance their cybersecurity resilience. Ongoing research and development are crucial to improving the framework and addressing new cybersecurity threats in the continuously evolving digital environment. In order for businesses to thrive in the digital era and safeguard their operations, reputation, and client trust, they must prioritize cybersecurity resilience. The ultimate significance of this framework lies in its capacity to reduce cyber risks, safeguard company assets, and ensure sustained security. This framework offers companies a tactical approach to maximizing cybersecurity resilience through the utilization of digitization capabilities [89,90]. To enhance the framework and address new cybersecurity challenges, further research and development in this field are imperative given the ever-changing digital ecosystem [91]. To thrive in the digital era and protect their operations, reputation, and clients, businesses must uphold cybersecurity resilience.

We anticipate that by incorporating these ideas into the proposed framework, companies will be better equipped to withstand cyberattacks and face the challenges of the digital era. This framework includes several strategies and offers comprehensive guidance to achieve excellence in cybersecurity defense. In the context of organizational operational transformation through digitization, new challenges related to cybersecurity arise as a secondary impact. Enhancing long-term security necessitates designing a cybersecurity resilience framework that integrates digitization capabilities. Our research outcomes underscore the vital role of digitization capabilities in various phases of cybersecurity resilience. The incorporation of diverse resources is crucial for training and prevention in cybersecurity resilience. We acknowledge the variation in information-sharing and process automation capabilities, prompting organizations to adopt appropriate digital solutions at critical junctures in their business processes. The efficient utilization of digital IT systems enables companies to respond swiftly and effectively to changing environments through strong improvisational capabilities.

Throughout the planning, preparation, and adaptation phases, we have identified relevant prevention, training, and review techniques. Online information capabilities support these steps. Update and improvisation emerge as pivotal mechanisms in addressing urgent environmental changes. This research underscores the importance of integrating digitization capabilities and cybersecurity resilience. A strong collaboration between the two will serve as a critical turning point in facing digital transformation. We believe that this collaboration will provide an advantage in addressing complex cybersecurity challenges and developing adaptive business strategies. While the proposed framework offers valuable guidance, we acknowledge the need for ongoing research and development to confront the evolving digital ecosystem. Only through sustained efforts can businesses successfully navigate digital transformation and maintain robust cybersecurity resilience against evolving cyber risks. By implementing these ideas within the proposed framework, we are confident that organizations will be better prepared to confront the challenges of the digital era and ensure their cybersecurity resilience with success.

The concepts we present in this article are depicted in Figure 9 below, which clearly illustrates how digitization capabilities and cybersecurity resilience can be integrated to create a comprehensive framework.

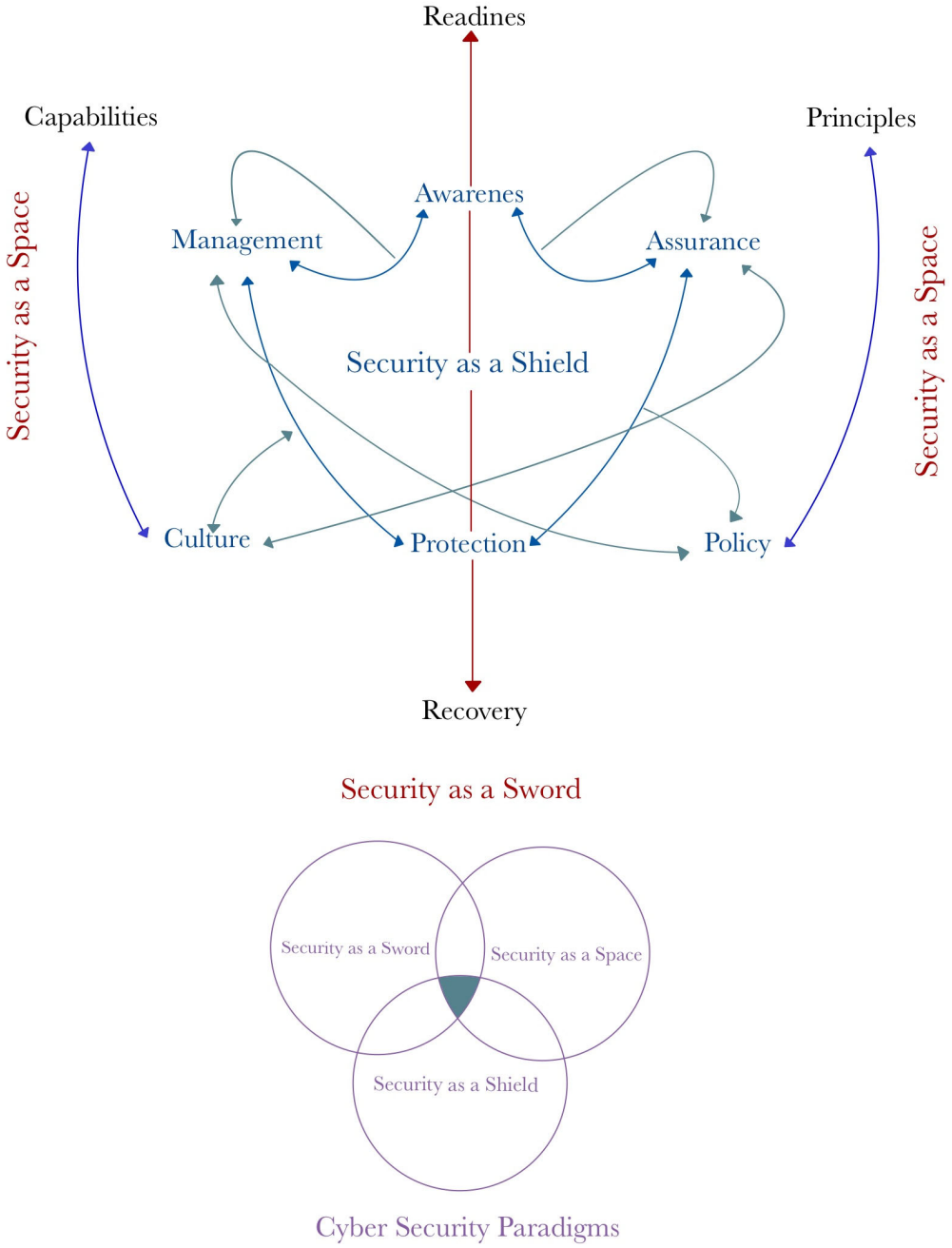

Figure 9. Cyber security paradigms.

(a) Security as a Shield

The concept of "Security as a Shield" involves four interconnected stages. First, Awareness ↔ Management indicates that an organization's awareness of cyber threats must be supported by effective management to oversee security. Sound management enables the organization to identify and prioritize necessary security measures. Second, Management ↔ Protection emphasizes that effective management should involve the implementation of adequate policies and protective measures to safeguard the organization's systems and data. Third, Protection ↔ Assurance underscores the importance of ensuring that the implemented protective measures are effective and in line with security standards. Lastly, Assurance ↔ Awareness reaffirms the need for ongoing security assessment and increasing awareness of cyber risks and responsibilities.

(b) Security as a Space

The concept of "Security as a Space" consists of two interconnected elements. First, Principles ↔ Policy indicates that the security principles underlying an organization should be reflected in clear security policies. These policies create a secure environment within the organization. Second, Capabilities ↔ Culture stresses the importance of developing adequate security capabilities and fostering a security culture throughout the organization. Security capabilities encompass the technology, processes, and human resources needed to create a safe and trustworthy environment.

(c) Security as a Sword

The concept of "Security as a Sword" involves two essential stages. First, Readiness emphasizes the importance of having a plan and infrastructure ready to confront cyber attacks. This readiness involves policies, technology, and personnel ready to act swiftly and effectively. Second, Recovery focuses on the organization's ability to quickly recover after an attack and restore normal operations. This recovery encompasses steps to restore systems, recover lost data, and reinstate services for users.

In this context, the concept of security can be categorized into three distinct paradigms: "Security as a Shield", "Security as a Space", and "Security as a Sword". Each paradigm comprises a set of interrelated steps and components that work together to form a comprehensive security plan. Within this framework, we will delve into the stages of each paradigm and present a carefully designed set of indicators. These indicators allow companies to quantitatively measure the effectiveness of their security approach. This measurement employs standard metrics with a rating scale from 5 (strong) to 1 (weak), providing an objective way to evaluate security processes and identify improvement opportunities. We will examine the relevant aspects of each paradigm and detail their measurements in Table 6.

Table 6. Cyber security paradigms framework.

No	Paradigm	Stage	Description
1.	Security as a Shield	Awareness ↔ Management	Organizational awareness of cyber threats supported by effective management strategies to address security.
		Management ↔ Protection	Implementation of policies and protective measures to safeguard systems and data.
		Protection ↔ Assurance	Ensuring effectiveness and compliance of protective measures with security standards.
		Assurance ↔ Awareness	Continuous security assessment and heightened awareness of cyber risks and responsibilities.
2.	Security as a Space	Principles ↔ Policy	Reflection of security principles in clear security policies to create a secure organizational environment.
		Capabilities ↔ Culture	Development of security capabilities and fostering a security culture within the organization.
3.	Security as a Sword	Readiness	Preparedness to face cyber attacks through ready policies, technologies, and personnel.
		Recovery	Swift recovery after attacks, restoring systems, recovering data, and reinstating user services.

Metrics for Assessment:

1. Security as a Shield Paradigm:

Table 7 presents a set of metrics that are central to the Security as a Shield paradigm, which focuses on establishing strong safeguards against cyberattacks. The paradigm con-

sists of several stages, starting with building awareness within the organization, followed by efficient management, implementing policies, taking proactive measures, and continuous evaluation. The table highlights key metrics such as the Security Awareness Index, Security Management Index, and Assurance Score. These metrics offer valuable insights into the organization's level of preparedness, effectiveness of management strategies, and commitment to implementing protective measures.

Table 7. Metrics for the security as a shield paradigm.

No	Metric	Description	Parameter				
			5	4	3	2	1
1.	Security Awareness Index (SAI)	Level of organizational awareness of cyber threats.	>80%	61–80%	41–60%	21–40%	<20%
2.	Security Management Index (SMI)	Effectiveness of security management actions.	>80%	61–80%	41–60%	21–40%	<20%
3.	Policy Compliance Rate (PCR)	Compliance level with security policies.	>80%	61–80%	41–60%	21–40%	<20%
4.	Protection Implementation Score	Effectiveness of implemented protective measures.	>80%	61–80%	41–60%	21–40%	<20%
5.	Compliance with Security Standards	Compliance of implemented protective measures.	>80%	61–80%	41–60%	21–40%	<20%
6.	Assurance Score (AS)	Effectiveness and compliance of protective measures via audits.	>80%	61–80%	41–60%	21–40%	<20%

2. Security as a Space Paradigm:

Table 8 outlines the metrics for the Security as a Space paradigm, which revolves around creating a secure environment through the integration of principles, rules, capabilities, and cultural aspects. This paradigm emphasizes the establishment of a secure space. The table introduces metrics such as the Policy Consistency Score and Security Capability Index. These metrics serve to gauge the alignment of security principles with organizational policies and the overall state of security readiness. In essence, the table provides a framework to assess how effectively security principles are integrated into the organization's operational practices within the context of this paradigm.

Table 8. Metrics for the security as a space paradigm.

No	Metric	Description	Parameter				
			5	4	3	2	1
1.	Policy Consistency Score (PCS)	Consistency of principles reflected in security policies.	>80%	61–80%	41–60%	21–40%	<20%
2.	Policy Compliance Rate (PCR)	Compliance level with security policies.	>80%	61–80%	41–60%	21–40%	<20%
3.	Security Capability Index (SCI)	Assessment of organizational security capabilities.	>80%	61–80%	41–60%	21–40%	<20%

3. Security as a Sword Paradigm:

Table 9 presents the metrics for the Security as a Sword paradigm, which underscores the importance of preparedness and adaptability in dealing with cyber attacks. This

paradigm centers around the concept of being ready to confront attacks and swiftly recuperating post-incident. The table introduces key metrics such as the Attack Readiness Score and Average Recovery Time. These metrics serve to assess an organization's capability to effectively handle and bounce back from cyber attacks. In essence, the table provides a concise framework to evaluate the organization's readiness and response strategies within the context of the Security as a Sword Paradigm.

Table 9. Metrics for the security as a sword paradigm.

No	Metric	Description	Parameter				
			5	**4**	**3**	**2**	**1**
1.	Attack Readiness Score (ARS)	Level of preparedness to respond to cyber attacks.	>80%	61–80%	41–60%	21–40%	<20%
2.	Average Recovery Time (RTO)	Average time to recover after a cyber attack.	<1 day	1–3 days	4–7 days	8–14 days	>14 days

Contributing to addressing evolving cybersecurity threats is a highly important step in maintaining digital security. Here are ten key actions you can take:

1. Increasing Awareness: Explaining the importance of cybersecurity to friends, family, and colleagues can help raise awareness about existing risks. This helps prevent actions that could worsen the situation.
2. Education and Training: Developing cybersecurity skills through training and education equips you with tools to protect yourself and your organization from security threats. You can take online courses, webinars, or utilize other available resources.
3. Engaging in the Cybersecurity Community: Joining local or online cybersecurity communities provides insights into the latest trends and threats, as well as opportunities to share knowledge and experiences.
4. Using Security Tools: Ensure your devices have up-to-date security software, including antivirus and firewalls. Regularly update to safeguard against evolving threats.
5. Practicing Digital Security: Implement digital security practices such as using strong and unique passwords for each account, employing two-factor authentication, and being cautious of suspicious links or attachments.
6. Reporting Suspicious Activity: If you observe suspicious activity or fall victim to an attack, promptly report it to relevant authorities or service providers.
7. Contributing to Research and Development: If you have a background in technology or security, you can contribute to researching and developing new solutions to address cybersecurity threats. This could involve creating new tools, methods, or approaches.
8. Sharing Information: Writing articles, blogs, or other educational content about cybersecurity practices or emerging trends can help disseminate valuable information to a wider audience.
9. Working in Cybersecurity: If you have a strong interest and aptitude in cybersecurity, consider working in the industry as a cybersecurity professional, researcher, or consultant.
10. Activism and Advocacy: Supporting policies and laws that promote cybersecurity protection, and engaging in cybersecurity awareness campaigns, are crucial steps in creating positive change in the digital environment.

Remember, small efforts from many individuals can have a significant impact on overall cybersecurity. Every step you take to contribute will help protect yourself, your organization, and society from evolving threats in the digital world.

Author Contributions: Conceptualization, M.F.S. and M.L.; methodology, M.F.S. and H.F.; Validation, M.L. and H.F.; formal analysis, M.F.S.; Investigation, M.F.S.; Resources, M.L. and H.F.; data curation, M.L.; writing-original draft preparation, M.F.S.; writing-review and editing, M.L. and H.F.; visualization, M.F.S.; supervision, M.L.; project administration, M.F.S.; funding acquisition, M.L. All authors have read and agreed to the published version of the manuscript.

Funding: The research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Jones, C.L.; Bridges, R.A.; Huffer, K.M.T.; Goodall, J.R. Towards a Relation Extraction Framework for Cyber-Security Concepts. In *ACM International Conference Proceeding Series*; Association for Computing Machinery: New York, NY, USA, 2015. [CrossRef]
2. Jeimy, J.; Cano, M. FLEXI—A Conceptual Model for Enterprise Cyber Resilience. *Procedia Comput. Sci.* **2023**, *219*, 11–19. [CrossRef]
3. Wallis, T.; Dorey, P. Implementing Partnerships in Energy Supply Chain Cybersecurity Resilience. *Energies* **2023**, *16*, 1868. [CrossRef]
4. Lubis, M.; Lubis, A.R. Designing Secured Cafe Network with Security Awareness Domain and Resource (SADAR) by Simulation using Cisco Packet Tracer. In *ACM International Conference Proceeding Series*; Association for Computing Machinery: New York, NY, USA, 2022; pp. 233–238. [CrossRef]
5. Bemthuis, R.; Iacob, M.-E.; Havinga, P. A Design of the Resilient Enterprise: A Reference Architecture for Emergent Behaviors Control. *Sensors* **2020**, *20*, 6672. [CrossRef] [PubMed]
6. Lubis, M.; Rahman, N.A.; Alam, P.F. Marketing Strategies Design for Crowdsourcing Application in Indonesia. In *ACM International Conference Proceeding Series*; Association for Computing Machinery: New York, NY, USA, 2021; pp. 25–31. [CrossRef]
7. Pieters, W.; Hadžiosmanović, D.; Dechesne, F. Cyber Security as Social Experiment. In *ACM International Conference Proceeding Series*; Association for Computing Machinery: New York, NY, USA, 2014; pp. 15–24. [CrossRef]
8. Lubis, M.; Fathoni, M.; Lubis, A.R. New Product Development Architectural Framework for Sustainability and Innovation within Telecommunication Industry. In *ACM International Conference Proceeding Series*; Association for Computing Machinery: New York, NY, USA, 2020; pp. 145–150. [CrossRef]
9. Grigaliūnas, Š.; Brūzgienė, R.; Venčkauskas, A. The Method for Identifying the Scope of Cyberattack Stages in Relation to Their Impact on Cyber-Sustainability Control over a System. *Electronics* **2023**, *12*, 591. [CrossRef]
10. Carías, J.F.; Labaka, L.; Sarriegi, J.M.; Hernantes, J. Defining a Cyber Resilience Investment Strategy in an Industrial Internet of Things Context. *Sensors* **2019**, *19*, 138. [CrossRef]
11. Kupsch, J.A.; Miller, B.P.; Heymann, E.; César, E. First principles vulnerability assessment. In Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop, Chicago, IL, USA, 8 October 2010; pp. 87–92.
12. Garcia-Perez, A.; Cegarra-Navarro, J.G.; Sallos, M.P.; Martinez-Caro, E.; Chinnaswamy, A. Resilience in healthcare systems: Cyber security and digital transformation. *Technovation* **2023**, *121*, 102583. [CrossRef]
13. Ademujimi, T.; Prabhu, V. Digital Twin for Training Bayesian Networks for Fault Diagnostics of Manufacturing Systems. *Sensors* **2022**, *22*, 1430. [CrossRef]
14. AlMajali, A.; Viswanathan, A.; Neuman, C. Resilience Evaluation of Demand Response as Spinning Reserve under Cyber-Physical Threats. *Electronics* **2017**, *6*, 2. [CrossRef]
15. Linkov, I.; Ligo, A.; Stoddard, K.; Perez, B.; Strelzoffx, A.; Bellini, E.; Kott, A. Cyber Efficiency and Cyber Resilience. *Commun. ACM* **2023**, *66*, 33–37. [CrossRef]
16. Hausken, K. Cyber resilience in firms, organizations and societies. *Internet Things* **2020**, *11*, 100204. [CrossRef]
17. Van Haastrecht, M.; Golpur, G.; Tzismadia, G.; Kab, R.; Priboi, C.; David, D.; Răcătăian, A.; Baumgartner, L.; Fricker, S.; Ruiz, J.F.; et al. A Shared Cyber Threat Intelligence Solution for SMEs. *Electronics* **2021**, *10*, 2913. [CrossRef]
18. Rizwan, K.; Ahmad, M.; Habib, M.A. Cyber Automated Network Resilience Defensive Approach against Malware Images. In *ACM International Conference Proceeding Series*; Association for Computing Machinery: New York, NY, USA, 2022; pp. 237–242. [CrossRef]
19. Kotenko, I.; Izrailov, K.; Buinevich, M.; Saenko, I.; Shorey, R. Modeling the Development of Energy Network Software, Taking into Account the Detection and Elimination of Vulnerabilities. *Energies* **2023**, *16*, 5111. [CrossRef]
20. Estay, D.A.S.; Sahay, R.; Barfod, M.B.; Jensen, C.D. A systematic review of cyber-resilience assessment frameworks. *Comput. Secur.* **2020**, *97*, 101996. [CrossRef]
21. Blay, K.B.; Yeomans, S.; Demian, P.; Murguia, D. The Information Resilience Framework. *J. Data Inf. Qual.* **2020**, *12*, 1–25. [CrossRef]
22. Jones, S.L.; Collins, E.I.M.; Levordashka, A.; Muir, K.; Joinson, A. What is 'cyber security'?: Differential language of cyber security across the lifespan. In Proceedings of the Conference on Human Factors in Computing Systems, Glasgow, UK, 4–9 May 2019; Association for Computing Machinery: New York, NY, USA, 2019; p. LBW0269. [CrossRef]

23. Staheli, D.; Yu, T.; Crouser, R.J.; Damodaran, S.; Nam, K.; O'Gwynn, D.; McKenna, S.; Harrison, L. Visualization evaluation for cyber security. In *ACM International Conference Proceeding Series*; Association for Computing Machinery: New York, NY, USA, 2014; pp. 49–56. [CrossRef]
24. Atighetchi, M.; Simidchieva, B.; Carvalho, M.; Last, D. Experimentation Support for Cyber Security Evaluations. In Proceedings of the 11th Annual Cyber and Information Security Research Conference, Oak Ridge, TN, USA, 5–7 April 2016; Association for Computing Machinery: New York, NY, USA, 2016. [CrossRef]
25. Abdullayeva, F. Cyber resilience and cyber security issues of intelligent cloud computing systems. *Results Control Optim.* **2023**, *12*, 100268. [CrossRef]
26. Nicholson, J.; McGlasson, J. CyberGuardians: Improving community cyber resilience through embedded peer-to-peer support. In Proceedings of the DIS 2020 Companion—Companion Publication of the 2020 ACM Designing Interactive Systems Conference, Eindhoven, The Netherlands, 6–10 July 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 117–121. [CrossRef]
27. Pham, L.N.H. Exploring Cyber-Physical Energy and Power System: Concepts, Applications, Challenges, and Simulation Approaches. *Energies* **2023**, *16*, 42. [CrossRef]
28. Lovatt, M. Herding cats: A case study on the development of Internet and intranet strategies within an engineering organization. In Proceedings of the 1997 ACM SIGCPR Conference on Computer Personnel Research, San Francisco, CA, USA, 3–5 April 1997; pp. 104–109.
29. Vasudevan, S.; Piazza, A.; Carr, M. Qualitative Factors in Organizational Cyber Resilience. In Proceedings of the International Conference on Cyber Resilience, ICCR 2022, Dubai, United Arab Emirates, 6–7 October 2022; pp. 1–5. [CrossRef]
30. Shreeve, B.; Gralha, C.; Rashid, A.; Araújo, J.; Goulão, M. Making Sense of the Unknown: How Managers Make Cyber Security Decisions. *ACM Trans. Softw. Eng. Methodol.* **2023**, *32*, 1–33. [CrossRef]
31. Berger, C.; Eichhammer, P.; Reiser, H.P.; Domaschka, J.; Hauck, F.J.; Habiger, G. A Survey on Resilience in the IoT. *ACM Comput. Surv.* **2022**, *54*, 1–39. [CrossRef]
32. Espinoza-Zelaya, C.; Moon, Y.B. Resilience Enhancing Mechanisms for Cyber-Manufacturing Systems against Cyber-Attacks. *IFAC-PapersOnLine* **2022**, *55*, 2252–2257. [CrossRef]
33. Cui, Y.; Idota, H. Improving Supply Chain Resilience with Establishing A Decentralized Information Sharing Mechanism. In *ACM International Conference Proceeding Series*; Association for Computing Machinery: New York, NY, USA, 2018; p. 23. [CrossRef]
34. Alby, M.F.; Ruslan, I.F.; Muharman, M.L. Information Security Test on Websites and Social Media Using Footprinting Method. In *ACM International Conference Proceeding Series*; Association for Computing Machinery: New York, NY, USA, 2022; pp. 521–525. [CrossRef]
35. Bauer, S.; Bernroider, E.W. From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *ACM SIGMIS Database DATABASE Adv. Inf. Syst.* **2017**, *48*, 44–68. [CrossRef]
36. Iannacone, M.; Bohn, S.; Nakamura, G.; Gerth, J.; Huffer, K.; Bridges, R.; Ferragut, E.; Goodall, J. Developing an Ontology for Cyber Security Knowledge Graphs. In *ACM International Conference Proceeding Series*; Association for Computing Machinery: New York, NY, USA, 2015; p. 12. [CrossRef]
37. Heck, H.; Kieselmann, O.; Wacker, A. Evaluating Connection Resilience for Self-Organizing Cyber-Physical Systems. In Proceedings of the IEEE 10th International Conference on Self-Adaptive and Self-Organizing Systems, SASO 2016, Augsburg, Germany, 12–16 September 2016; pp. 140–141. [CrossRef]
38. Mohamed, N.; Salama, M.M.A. Data Mining-Based Cyber-Physical Attack Detection Tool for Attack-Resilient Adaptive Protective Relays. *Energies* **2022**, *15*, 4328. [CrossRef]
39. Niu, L.; Al Maruf, A.; Clark, A.; Mertoguno, J.S.; Poovendran, R. POSTER: A Common Framework for Resilient and Safe Cyber-Physical System Design. In Proceedings of the ACM Asia Conference on Computer and Communications Security, New York, NY, USA, 10–14 July 2023; pp. 1025–1027. [CrossRef]
40. Choudhury, S.; Rodriguez, L.; Curtis, D.; Oler, K.; Nordquist, P.; Chen, P.-Y.; Ray, I. Action Recommendation for Cyber Resilience. In Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense, Denver, CO, USA, 12 October 2015; pp. 3–8. [CrossRef]
41. Camilli, M.; Mirandola, R.; Scandurra, P. Enforcing Resilience in Cyber-physical Systems via Equilibrium Verification at Runtime. *ACM Trans. Auton. Adapt. Syst.* **2023**. [CrossRef]
42. Bridges, S.M.; Keiser, K.; Sissom, N.; Graves, S.J. Cyber Security for Additive Manufacturing. In *ACM International Conference Proceeding Series*; Association for Computing Machinery: New York, NY, USA, 2015. [CrossRef]
43. Shaked, A.; Tabansky, L.; Reich, Y. Incorporating Systems Thinking into a Cyber Resilience Maturity Model. *IEEE Eng. Manag. Rev.* **2020**, *49*, 110–115. [CrossRef]
44. Baho, S.A.; Abawajy, J. Analysis of Consumer IoT Device Vulnerability Quantification Frameworks. *Electronics* **2023**, *12*, 1176. [CrossRef]
45. Mohammadi, F. Emerging Challenges in Smart Grid Cybersecurity Enhancement: A Review. *Energies* **2021**, *14*, 1380. [CrossRef]
46. Santos, H.; Oliveira, A.; Soares, L.; Satis, A.; Santos, A. Information Security Assessment and Certification within Supply Chains. In Proceedings of the 16th International Conference on Availability, Reliability and Security, Vienna, Austria, 17–20 August 2021; pp. 1–6.

47. Haya, G.M. Complexity reduction in information security risk assessment. In Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research, Newport Beach, CA, USA, 4–6 June 2015; pp. 5–6.
48. Bennaceur, A.; Ghezzi, C.; Tei, K.; Kehrer, T.; Weyns, D.; Calinescu, R.; Dustdar, S.; Hu, Z.; Honiden, S.; Ishikawa, F.; et al. Modelling and Analysing Resilient Cyber-Physical Systems. In Proceedings of the 2019 IEEE/ACM 14th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS), Montreal, QC, Canada, 25 May 2019; pp. 70–76. [CrossRef]
49. Kong, F.; Xu, M.; Weimer, J.; Sokolsky, O.; Lee, I. Cyber-Physical System Checkpointing and Recovery. In Proceedings of the 2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS), Porto, Portugal, 11–13 April 2018; pp. 22–31. [CrossRef]
50. Thorpe, J.; Fasano, R.; Sahakian, M.G.; Gonzales, A.; Hahn, A.; Morris, J.; Ortiz, T.; Reinbolt, H.; Vugrin, E.D. A Cyber-Physical Experimentation Platform for Resilience Analysis. In Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, Baltimore, MD, USA, 27 April 2022; pp. 3–12. [CrossRef]
51. Bucur, V.; Miclea, L.-C. Multi-Cloud Resource Management Techniques for Cyber-Physical Systems. *Sensors* **2021**, *21*, 8364. [CrossRef]
52. Patriarca, R.; Simone, F.; Di Gravio, G. Modelling cyber resilience in a water treatment and distribution system. *Reliab. Eng. Syst. Saf.* **2022**, *226*, 108653. [CrossRef]
53. Zhu, C.; Wu, J.; Liu, M.; Luan, J.; Li, T.; Hu, K. Cyber-physical resilience modelling and assessment of urban roadway system interrupted by rainfall. *Reliab. Eng. Syst. Saf.* **2020**, *204*, 107095. [CrossRef]
54. Rahman, S.; Hossain, N.U.I.; Govindan, K.; Nur, F.; Bappy, M. Assessing cyber resilience of additive manufacturing supply chain leveraging data fusion technique: A model to generate cyber resilience index of a supply chain. *CIRP J. Manuf. Sci. Technol.* **2021**, *35*, 911–928. [CrossRef]
55. Kesswani, N.; Kumar, S. Maintaining cyber security: Implications, cost and returns. In Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research, Newport Beach, CA, USA, 4–6 June 2015; pp. 161–164. [CrossRef]
56. Pavão, J.; Bastardo, R.; Carreira, D.; Rocha, N.P. Cyber Resilience, a Survey of Case Studies. *Procedia Comput. Sci.* **2023**, *219*, 312–318. [CrossRef]
57. Colabianchi, S.; Costantino, F.; Di Gravio, G.; Nonino, F.; Patriarca, R. Discussing resilience in the context of cyber physical systems. *Comput. Ind. Eng.* **2021**, *160*, 107534. [CrossRef]
58. Cheng, E.; Gritschneder, D.M.; Abraham, J.; Bose, P.; Buyuktosunoglu, A.; Chen, D.; Cho, H.; Li, Y.; Sharif, U.; Skadron, K.; et al. Cross-layer resilience: Challenges, insights, and the road ahead. In Proceedings of the 56th Annual Design Automation Conference, Las Vegas, NV, USA, 2–6 June 2019. [CrossRef]
59. Gupta, K.; Sahoo, S.; Panigrahi, B.K.; Blaabjerg, F.; Popovski, P. On the Assessment of Cyber Risks and Attack Surfaces in a Real-Time Co-Simulation Cybersecurity Testbed for Inverter-Based Microgrids. *Energies* **2021**, *14*, 4941. [CrossRef]
60. Khalghani, M.R.; Verma, V.; Solanki, S.K.; Solanki, J.M. Resilient Networked Control of Inverter-Based Microgrids against False Data Injections. *Electronics* **2022**, *11*, 780. [CrossRef]
61. Czejdo, B.D.; Iannacone, M.D.; Bridges, R.A.; Ferragut, E.M.; Goodall, J.R. Integration of external data sources with cyber security data warehouse. In *ACM International Conference Proceeding Series*; Association for Computing Machinery: New York, NY, USA, 2014; pp. 49–52. [CrossRef]
62. Doynikova, E.; Fedorchenko, A.; Kotenko, I. Ontology of Metrics for Cyber Security Assessment. In *ACM International Conference Proceeding Series*; Association for Computing Machinery: New York, NY, USA, 2019. [CrossRef]
63. Safitra, M.F.; Abdurrahman, L. Open-up International Market Opportunities: Using the OSINT Crawling and Analyzing Method. *SEIKO J. Manag. Bus.* **2023**, *6*, 923–931.
64. *ISO 27001*; Information Security Management Systems. ISO: Geneva, Switzerland, 2022.
65. Kim, S.; Kim, D. Securing the Cyber Resilience of a Blockchain-Based Railroad Non-Stop Customs Clearance System. *Sensors* **2023**, *23*, 2914. [CrossRef]
66. Toh, J.; Hatib, M.; Porzecanski, O.; Elovici, Y. Cyber security patrol: Detecting fake and vulnerable wifi-enabled printers. In Proceedings of the Symposium on Applied Computing, Marrakech, Morocco, 3–7 April 2017; pp. 535–542. [CrossRef]
67. Murdoch, S.; Leaver, N. Anonymity vs. Trust in Cyber-Security Collaboration. In Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, co-located with: CCS 2015, Denver, CO, USA, 12 October 2015; pp. 27–29. [CrossRef]
68. Wu, Q.; Zhang, H.; Pu, J. Mitigating distributed denial-of-service attacks using network connection control charts. In Proceedings of the 2nd International ICST Conference on Scalable Information Systems, Suzhou, China, 5–7 June 2007.
69. Alnaim, A.K.; Alwakeel, A.M.; Fernandez, E.B. A Misuse Pattern for Distributed Denial-of-Service Attack in Network Function Virtualization. In Proceedings of the 26th PLoP'19, Ottawa, ON, Canada, 7–10 October 2019.
70. Safitra, M.F.; Lubis, M.; Widjajarto, A. Security Vulnerability Analysis using Penetration Testing Execution Standard (PTES): Case Study of Government's Website. In Proceedings of the 2023 6th International Conference on Electronics, Communications and Control Engineering, Fukuoka, Japan, 24–26 March 2023; pp. 139–145. [CrossRef]
71. Nykänen, R.; Kärkkäinen, T. Supporting Cyber Resilience with Semantic Wiki. In Proceedings of the 12th International Symposium on Open Collaboration, OpenSym 2016, Berlin, Germany, 17–19 August 2016. [CrossRef]

72. Khan, Y.I.; Al-Shaer, E.; Rauf, U. Cyber resilience-by-construction: Modeling, measuring & verifying. In Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense, Denver, CO, USA, 12 October 2015; pp. 9–14. [CrossRef]
73. Georgiadou, A.; Michalitsi-Psarrou, A.; Askounis, D. Cyber-Security Culture Assessment in Academia: A COVID-19 Study: Applying a Cyber-Security Culture Framework to assess the Academia's resilience and readiness. In *ACM International Conference Proceeding Series*; Association for Computing Machinery: New York, NY, USA, 2022. [CrossRef]
74. Belaid, Y.N.; Coudray, P.; Sanchez-Torres, J.; Fang, Y.-P.; Zeng, Z.; Barros, A. Resilience Quantification of Smart Distribution Networks—A Bird's Eye View Perspective. *Energies* **2021**, *14*, 2888. [CrossRef]
75. Bellini, E.; Marrone, S.; Marulli, F. Cyber Resilience Meta-Modelling: The Railway Communication Case Study. *Electronics* **2021**, *10*, 583. [CrossRef]
76. Barzegari, Y.; Zarei, J.; Razavi-Far, R.; Saif, M.; Palade, V. Resilient Consensus Control Design for DC Microgrids against False Data Injection Attacks Using a Distributed Bank of Sliding Mode Observers. *Sensors* **2022**, *22*, 2644. [CrossRef]
77. Welsh, T.; Benkhelifa, E. On Resilience in Cloud Computing. *ACM Comput. Surv.* **2020**, *53*, 1–36. [CrossRef]
78. Rodriguez, L.; Curtis, D.; Choudhury, S.; Oler, K.; Nordquist, P.; Chen, P.-Y.; Ray, I. DEMO: Action recommendation for cyber resilience. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, 12–16 October 2015; pp. 1620–1622. [CrossRef]
79. Liang, X.; Konstantinou, C.; Shetty, S.; Bandara, E.; Sun, R. Decentralizing Cyber Physical Systems for Resilience: An Innovative Case Study from A Cybersecurity Perspective. *Comput. Secur.* **2023**, *124*, 102953. [CrossRef]
80. Attajer, A.; Chaabane, S.; Darmoul, S.; Sallez, Y.; Riane, F. Evaluation of Operational Resilience in Cyber-Physical Production Systems: Literature review. *IFAC-PapersOnLine* **2022**, *55*, 2264–2269. [CrossRef]
81. Farraj, A.; Hammad, E.; Kundur, D. Impact of Cyber Attacks on Data Integrity in Transient Stability Control. In Proceedings of the 2017 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids, CPSR-SG 2017 (Part of CPS Week), Pittsburgh, PA, USA, 18–21 April 2017; pp. 29–34. [CrossRef]
82. Sapra, V.; Hasan, M.K.; Ghazal, T.M.; Bhadrdwaj, A.; Bharany, S.; Ahmad, M.; Rehman, A.U.; Mohamed, T. Privacy-based framework for Cyber Resilience of Healthcare based data for use with Machine Learning algorithms. In Proceedings of the 2022 International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 6–7 October 2022; pp. 1–6. [CrossRef]
83. Rimawi, D. Green Resilience of Cyber-Physical Systems. In Proceedings of the 2022 IEEE International Symposium on Software Reliability Engineering Workshops, Charlotte, NC, USA, 31 October–3 November 2022; pp. 105–109. [CrossRef]
84. Safitra, M.F.; Lubis, M.; Kurniawan, M.T. Cyber Resilience: Research Opportunities. In Proceedings of the 2023 6th Inter-National Conference on Electronics, Communications and Control Engineering, Fukuoka, Japan, 24–26 March 2023. [CrossRef]
85. Hromada, M.; Rehak, D.; Lukas, L. Resilience Assessment in Electricity Critical Infrastructure from the Point of View of Converged Security. *Energies* **2021**, *14*, 1624. [CrossRef]
86. Nguyen, T.; Wang, S.; Alhazmi, M.; Nazemi, M.; Estebsari, A.; Dehghanian, P. Electric Power Grid Resilience to Cyber Adversaries: State of the Art. *IEEE Access* **2020**, *8*, 87592–87608. [CrossRef]
87. Valinejad, J.; Mili, L. Community Resilience Optimization Subject to Power Flow Constraints in Cyber-Physical-Social Systems. *IEEE Syst. J.* **2022**, *17*, 2904–2915. [CrossRef]
88. Dupont, B.; Shearing, C.; Bernier, M.; Leukfeldt, R. The tensions of cyber-resilience: From sensemaking to practice. *Comput. Secur.* **2023**, *132*, 103372. [CrossRef]
89. Osborn, J.K.; Sepulveda-Estay, D.A. A Comparative Analysis of the Impact-Wave Analogy Cyber-Resilience Framework. In Proceedings of the 2021 IEEE International Conference on Industrial Engineering and Engineering Management, Singapore, 13–16 December 2021; pp. 333–337. [CrossRef]
90. Ng, D.J.X.; Easwaran, A.; Andalam, S. Contract-based hierarchical resilience framework for cyber-physical systems. In Proceedings of the 2019 ACM/IEEE International Conference on Cyber-Physical Systems, Montreal, QC, Canada, 16–18 April 2019; pp. 324–325. [CrossRef]
91. Kolosok, I.; Gurina, L. Cyber resilience models of systems for monitoring and operational dispatch control of electric power systems. *IFAC-PapersOnLine* **2022**, *55*, 485–490. [CrossRef]