Cyber Capabilities as Dynamic Capabilities: Meeting the Demands of the Ever-Evolving Cybersecurity Environment

Nico Abbatemarco
SDA Bocconi School of Management
nico.abbatemarco@sdabocconi.it

Abstract

Despite the growing importance of cybersecurity, a lack of theoretical studies hampers a comprehensive understanding of this field. This gap becomes particularly evident when attempting to investigate the impacts of cybersecurity on organizational performance. To address this gap, this paper conducts a Systematic Literature Review (SLR) to identify a series of core cybersecurity capabilities and applies the dynamic capabilities framework to analyze them. The study categorizes the 17 identified capabilities into sense, seize, and transform clusters, exploring their contributions to organizational performance and their interrelationships. While many of these capabilities align with established cybersecurity standards such as ISO 27001 and NIST CSF, the findings emphasize specifically the critical role played by less technical and more strategic-oriented capabilities. This research represents an initial step in bridging the existing knowledge gap and offers valuable insights for future investigations into the microfoundations and evolving nature of dynamic cyber capabilities.

Keywords: Cybersecurity, Cybersecurity Strategy, Cybersecurity Capabilities, Dynamic Capabilities, Organizational Performance

1. Introduction

In today's digital age – and especially after the COVID-19 pandemic – organizations across industries and sectors are increasingly reliant on information and digital technologies to conduct their daily activities (Leonardi, 2021; Peppard & Ward, 2016). However, this reliance also brings the inherent risk of cyber threats that can exploit vulnerabilities in these systems, resulting in significant financial losses, reputational damage, and potential legal consequences (Stouffer et al., 2019). The cyber space has witnessed a rapid evolution in recent years – with cyber-attacks becoming more frequent, sophisticated, and destructive (Lallie et al., 2021; Weil & Murugesan, 2020) – and the continuous evolution of enterprise IT architectures is introducing additional complexities. The current cost of global cybercrime was estimated at 6 trillion USD at the end of 2021, nearly doubling from five years earlier. In the same time frame, global cybersecurity spending grew nearly tenfold, from 100 billion USD to 1 trillion USD (Morgan, 2018). In this highly dynamic context, cybersecurity is slowly but significantly influencing the traditional way of conducting business operations in different sectors (Abbatemarco et al., 2022; Carcary et al., 2019).

Despite significant investments in cybersecurity technologies and resources, many organizations still struggle to effectively protect their assets and respond to evolving threats (Kosutic & Pigni, 2020; Sen, 2018). One key contributing factor to this challenge lies in the lack of clear recognition and understanding of the core cybersecurity capabilities (Kosutic & Pigni, 2020). These capabilities should reflect the organization's ability to convert the imperative to address cyber risks into managerial decisions that not only support, but also enhance overall business performances. In this sense, these capabilities bear resemblance to the concept of dynamic capabilities, defined by Teece et al. (1997) as the *"organization's ability to integrate, build, and reconfigure internal and external competences to address rapidly changing environments"*.

The concept of dynamic capabilities has been frequently employed in the strategic management literature to explain how organizations can gain a competitive advantage by quickly identifying and seizing new opportunities, responding to market shifts, and effectively navigating through volatile, uncertain, complex and ambiguous scenarios (Eisenhardt & Martin, 2000; Teece, 2007; Teece et al., 1997). Although one could argue that cybersecurity does not directly confer a competitive edge, as it is not inherently tied to competition among organizations and instead emphasizes collaboration between them (Pala & Zhuang, 2019; Sharkov, 2016), maintaining a strong cybersecurity posture is undeniably vital for at least preserving the current competitive advantages. This

entails, for example, safeguarding the organization's assets, ensuring uninterrupted operations, and thereby upholding the trust of customers, partners, and other stakeholders (Craigen et al., 2014; Salviotti et al., 2023; Weil & Murugesan, 2020). Additionally, cybersecurity might also create new competitive advantages, such as by attracting prospective customers who favor products / services adhering to strict privacy policies (Rothrock et al., 2018).

Despite the relevance of the topic, understanding what dynamic capabilities are required in the cybersecurity domain is challenging. Formulating a comprehensive and coherent list of capabilities is intricate due to several factors. One is the fragmented state of academic literature regarding the subject, which, although gaining significance, remains notably compartmentalized across its technical, organizational, and legal dimensions. Other factors are the novelty and dynamism of the field itself: cybersecurity is a multifaceted and dynamic domain, that demands continuous adaptation from organizations to address emerging threats and vulnerabilities (Craigen et al., 2014; Suryotrisongko & Musashi, 2019). Today's cybersecurity landscape is shaped by several influencing forces, such as technological advancements and new regulations (Madnick et al., 2023; Willard, 2015). A third factor is that the two most recognized cybersecurity frameworks, the ISO 27001 and the NIST Cybersecurity Framework (NIST CSF), have de facto established their own list of required cyber capabilities. Despite their undeniable usefulness for organizations (Podrecca et al., 2022; Scofield, 2016), referring exclusively to these two frameworks bring the risk of overlooking capabilities that they do not highlight, or overemphasizing or underestimating others.

To implement effective cybersecurity strategies, it is reasonable to assume that organizations should thoroughly and comprehensively understand the capabilities required to address this dynamic landscape. In light of this observation, the primary objective of this paper is to address the following key research question:

RQ. What are the dynamic capabilities that organizations need to effectively address the rapidly changing cybersecurity environment?

To accomplish this goal, the study employs a systematic literature review (SLR) methodology to rigorously identify and collect existing research on cybersecurity capabilities. The findings of the SLR are then synthesized using a thematic synthesis approach (Thomas & Harden, 2008; Xiao & Watson, 2019), and finally analyzed through the Dynamic Capabilities framework according to Teece et al. (1997).

The following sections of the paper are organized as follows. Section 2 provides an overview of the theoretical underpinnings behind the relevance of cybersecurity today and the dynamic capabilities theory. Section 3 details the methodology and process employed in conducting the SLR, including the search strategy, inclusion criteria, and data analysis techniques. Section 4 presents the findings of the review, identifying the dynamic capabilities that organizations require to effectively handle cybersecurity. Section 5 discusses the consequences of these findings, drawing connections to traditional dynamic capabilities and emphasizing their practical implications for organizations. Finally, Section 6 offers concluding remarks, highlights the contributions of the study, and suggests avenues for future research.

2. Theoretical background

2.1 Relevance of cybersecurity

As mentioned in the introduction, the growing pervasiveness of digital technologies in companies is leading to a profound change in the information security paradigm (Leonardi, 2021; Peppard & Ward, 2016). Organizations are exposed to an unprecedented amount of cyber risks, defined as the risks *"of financial loss, operational disruption, or damage"* resulting from *"the unauthorized access, use, disclosure, disruption, modification, or destruction of [an information] system"* (Stouffer et al., 2019, p.70). In addition, these risks often go beyond the perimeter covered by traditional Information Security Management Systems (Craigen et al., 2014; Schatz et al., 2017). In 2013, von Solms & van Niekerk were among the first to claim that information security and cybersecurity were related, but not analogous terms: while traditional Information Security has as its main purpose *"the protection of the corporate information technology infrastructure"* and of *"all the information that is not stored or communicated directly using ICT"*, cybersecurity has a wider scope, that goes beyond the traditional perimeter of the company. In this sense, in cybersecurity *"the assets that need to be protected can range from the person him/herself […] to the interests of society at large"*(von Solms & van Niekerk, 2013, pp. 101–102). Cybersecurity can include activities such as protecting employees even outside the corporate environment (He & Zhang, 2019), preventing and communicating potential cyber risks with the company's 3rd- and 4th-parties (Levy & Gafni, 2021), ensuring the cyber-safety of a product for a certain period of time after its sale (Chhetri et al., 2018), and coordinating with the national security and privacy authorities in case of a cyber incident (Sabillon et al., 2016). As a result, cybersecurity is today a strategic Board- and CEO-level issue, rather than simply an IT one.

2.2 The dynamic capabilities framework

In the ever-changing and competitive business landscape, organizations are constantly challenged to adapt and respond to dynamic environments. The concept of dynamic capabilities has emerged as a prominent theoretical framework to understand how organizations can effectively navigate and thrive in such turbulent conditions (Eisenhardt & Martin, 2000; Helfat & Peteraf, 2009; Peteraf et al., 2013; Teece, 2007; Teece et al., 1997). Dynamic capabilities represent the "*ability to integrate, build, and reconfigure internal and external competences to address rapidly changing environments"* (Teece et al., 1997).

The concept of dynamic capabilities has gained significant attention across various disciplines, including strategic management, organizational theory, and innovation studies. It extends the traditional resource-based view (RBV) of the firm by emphasizing the importance of capabilities and processes that enable firms to adapt and shape their resource base (Eisenhardt & Martin, 2000). Dynamic capabilities encompass a set of organizational routines and processes that facilitate sensing, seizing, and reconfiguring resources in response to changing market conditions (Teece, 2007).

The three core dimensions of dynamic capabilities – sensing, seizing, and transforming – form the foundation of the original conceptual framework. Sensing capabilities involve scanning and interpreting the external environment to identify emerging opportunities and threats. Seizing capabilities refer to an organization's ability to rapidly and effectively capture and exploit identified opportunities. Finally, transforming capabilities encompass the ability to internally reallocate and recombine its resources and capabilities in response to changing market dynamics.

2.3 Research gap

Given the relevance of the topic, in recent years several research streams have begun exploring how cybersecurity can be leveraged to protect or even improve business performance. Works in the field of computer science and information technology were the first to explore the impact of cybersecurity, with both academic and practitioner articles primarily focusing on the technical capabilities needed to address its challenges, and with some authors already providing early organizational perspectives (e.g., Adler, 2013; Donaldson et al., 2015; Jang-Jaccard & Nepal, 2014).

Starting from 2017-2018, several works started presenting a more holistic viewpoint on the matter, often coming from Chief Information Security Officers (CISOs), former CISOs, and other experienced security professionals (see for example Antonucci, 2017). Through practical guidance, best practices, and lessons learned from their personal careers, these publications started suggesting that cybersecurity capabilities should encompass a broad range of technical, managerial, and legal practices. Many of these works were also influenced by the rise of international standards in the cybersecurity domain, particularly after 2013 with the release of globally accepted frameworks such as ISO 27001 or NIST CSF. The widespread adoption of these frameworks effectively standardized a set of capabilities across different sectors and geographies. In its latest edition, the ISO 27001:2022 presents cybersecurity activities in the form of 8 main "clauses": Context of the Organization, Leadership, Planning, Support, Operation, Performance Evaluation, and Improvement (ISO, 2022). On the other side, the latest revision of the NIST CSF (Barrett, 2018) identifies five core "functions": Identify, Protect, Detect, Respond and Recover. The main gaps in this organization-oriented research stream are twofold: on one hand, a pronounced emphasis placed on the capabilities identified and described by these standards, and on the other hand, a bias related to the authors' professional experiences.

A third research stream, back in the academic realm, primarily focused on how to develop the cybersecurity capabilities identified in the models and maturity frameworks mentioned above (e.g., Almuhammadi & Alsaleh, 2017; Jacobs et al., 2016). Lastly, a fourth and most recent research stream tried to understand what new needs emerged following the latest changes in the cyber landscape, including the increase in global cyber-attacks recorded since the Covid-19 pandemic and the release of several national and international security laws and regulations (Lallie et al., 2021; Srinivas et al., 2019). One of the most relevant works in this latest stream – characterized by a less technologically- and more strategically-oriented approach to cybersecurity – is that by Kosutic & Pigni (2020), who were among the first to consider cyber capabilities as akin to dynamic capabilities as described by Teece et al. (1997). The choice of the dynamic capabilities framework is indeed highly congruent with the current cybersecurity environment, given its primary objective of investigating an organization's ability to promptly adapt strategies and structures in response to the rapid evolution of the market to maintain its competitive advantage (Helfat & Peteraf, 2009). In particular, Kosutic and Pigni (2020) were the first to recognize how the dimensions delineated by Teece et al. (1997) inherently align with the demands imposed by the present context. For instance, their work identifies the capability to "sense" emerging threats and vulnerabilities, to "seize" opportunities to enhance defenses, and to "transform" security strategies and technologies. This alignment further underscores the fit

of the framework to this domain, where the need to perceive and respond to swiftly evolving threats is paramount. However, even Kosutic & Pigni's work lacks proper systematization, having been *"built by merging existing academic literature and evidence from the field"*, also thanks to *"the professional experience of the first author as a cybersecurity expert"* (p.35). Again, while this approach may be highly valuable from a practical perspective, it is also likely to have overlooked or underestimated significant cyber capabilities mentioned by other sources.

To summarize, all the different research streams on cybersecurity capabilities still lack a proper systematization and classification. The aim of this study is to methodically identify the cyber capabilities needed today to address the rapidly changing cybersecurity environment and frame them within a broader model of dynamic capabilities as described by Teece et al. (1997).

3. Methodology

For the systematic literature review, the paper followed the procedure proposed by Tranfield et al. (2003), particularly following the revised version by Xiao & Watson (2019) that incorporates the revisions from Brereton et al. (2007) and Kitchenham & Charters (2007). The procedure encompassed three main stages: planning, conducting, and reporting the review. During the planning stage, a review protocol was established. Firstly, the purpose of the review was defined, which led to the definition of the RQ. Subsequently, inclusion and exclusion criteria were selected. For the purposes of this SLR, only works that dealt with how cybersecurity can contribute to business performance were considered. The publication timeframe for the selected works ranged from 2013 to 2023, reflecting the emphasis on today's cybersecurity landscape. Finally, considering the focus of the work, the paper incorporated both quantitative and qualitative publications, including case studies.

The search strategy began by creating search strings that were then combined to form keywords. Wildcard symbols were also employed during the search to reduce the number of strings. Three sets of keywords were used, the first being "cybersecurity" OR "cyber security" OR "information security" OR "infosec". The reason for such set is that, although cybersecurity and information security cannot be considered synonymous, they have been and are still often used interchangeably. The second and third sets of keywords were selected following an approach analogous to Mikalef et al. (2018), that engaged a panel of experts to determine the most pertinent keyword set for a SLR that investigated dynamic capabilities in a technologically-driven context. Similar to their work, the second set thus included the words "capabilities" OR "competencies" OR "practices" OR "resource-based view", while the third one included only a single term: "performance".

In the conducting phase, the search strategy was initially performed on the Web of Science (477 results) and Scopus databases (940 results). Keywords were searched within the title, abstract, and keyword sections of the manuscripts. Subsequently, the search was repeated on the IEEE Xplore database (1,099 results) and on the Association of Information Systems library (351 results), where the search was extended to all metadata. Finally, the search was also performed on Google Scholar using the Publish or Perish software, which yielded 1,004 results. In total, at this stage the search yielded 3,871 results, which were soon reduced to 793 after removing duplicates, non-English papers, books and articles published on non-scientific outlets. The titles of the selected studies were then analyzed to determine their relevance to the systematic review. Studies that were clearly not about the business or organizational impacts of cybersecurity were excluded at this point. After this stage, the number of remaining articles was 214. In the second stage, the abstracts of the remaining articles were examined; those that did not align with the focus of the review were discarded, as well as papers with a different unit of analysis than that indicated in the research question (e.g., focusing on individual capabilities rather than organizational ones). Furthermore, in-progress papers and thesis dissertations were excluded. Out of the 214 abstracts assessed, 128 were omitted, leaving 86 papers for further analysis. In the third stage, each of the 86 remaining papers was evaluated based on several quality criteria, including scientific rigor and credibility. At this stage, an additional 41 papers were excluded, leaving 45 papers for data extraction and synthesis. The whole process is summarized in Figure 1 below.

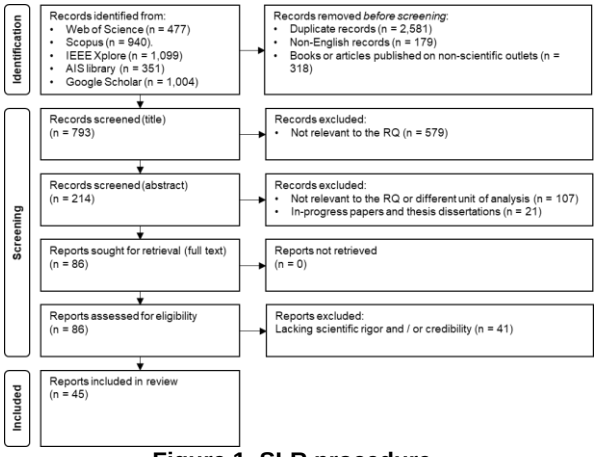

Figure 1. SLR procedure.

In terms of publication counts, the final records encompass 26 journal articles and 19 articles from

conference proceedings. Among journals, the most represented publications are Information & Computer Security (Emerald Publishing) with 4 entries and Computers & Security (Elsevier) with 3. Among conferences, the most represented are the European Conference on Information Warfare and Security (ECCWS) with 4 records, the Hawaii International Conference on System Sciences (HICSS) with 3, and the Americas' Conference on Information Systems (AMCIS) with 2. All other outlets have only 1 entry each. In terms of time distribution, the years with the highest representation are 2021 and 2022, with 8 records each, followed by 2019 and 2020 with 6. The earliest entry is dated 2013, the most recent May 2023.

In order to achieve consistency in the extracted data, a thematic synthesis approach based on Thomas & Harden (2008) was adopted. In thematic synthesis, initial themes are extracted from the literature and then clustered and further synthesized into analytical themes that are relevant to address a specific research question. According to Thomas and Harden (2008), analytical themes are particularly suitable when addressing a specific review question, which aligns well with the purpose of this paper. After the synthesis, each of the identified analytical themes was linked to one of the three original dynamic capabilities identified by Teece et al. (1997). The final outcomes of the data collection, extraction, synthesis, and analysis are presented in the subsequent section.

4. Findings

This section presents the results of the systematic literature review. From the synthesis process, 17 dynamic cyber capabilities emerged, which were then analyzed and redistributed into the three macro clusters of sensing, seizing, and transforming capabilities, as theorized by Teece et al. (1997):

- "Sense" cluster: capabilities related to sensing and identifying new opportunities and potential threats in the external environment.
- "Seize" cluster: capabilities related to seizing and capturing these opportunities effectively.
- "Transform" cluster: capabilities related to transforming and reconfiguring internal resources, processes, and capabilities to adapt to new opportunities or threats.

The results are presented in Table 1 in the following page. In addition to indicating the cluster, the table provides a brief description of what each capability involves and its goal, along with the number of papers that mentioned it and some references (due to space constraints, only three per capability are shown). In terms of cluster mentions, "Seize" capabilities are cited in 42 out of the 45 examined papers, "Sense" capabilities in 37, while "Transform" ones in 31. In total, the dynamic capabilities related to the "Sense" cluster are cited 78 times, those related to the "Seize" cluster 134 times, and those related to the "Transform" cluster 45 times.

5. Discussion

5.1 Overview of cyber capabilities

The findings imply the existence of different capabilities' domains, reinforcing the concept of cybersecurity as a multidisciplinary subject. The identified capabilities have been categorized into five primary groups according to their overarching domains, as represented in Figure 2.

Domain	Sense		Seize		Transform	
Strategy & Governance	ID VI. Identifying and prioritizing cyber risks	ID XIII. Monitoring 3rd-party cyber risks	ID I. Setting up a comprehensive strategy & governance structure	ID X. Monitoring and evaluating cybersecurity performances	ID XVII. Understanding the cybersecurity needs of customers	
Architecture & Tools	ID XI. Selecting and integrating new technologies		ID II. Building and managing the core cybersecurity architecture	ID XIV. Integrating cybersecurity and physical security	ID XII. Making cybersecurity closer to the users	
Training & Awareness			ID V. Fostering internal and external cybersecurity awareness		ID III. Fostering the development of cybersecurity skills	ID XVI. Implementing security in HR practices
Incident Prevention & Response	ID IV. Enhancing threat prevention	ID XV. Collaborating with external entities	ID VIII. Managing incident response		ID IX. Developing pervasive security operations	
Compliance			ID VII. Enforcing compliance to laws, regulations, standards			

Figure 2. Categorization of capabilities.

Starting from the first group, the most cited capability is "Setting up a comprehensive strategy & governance structure" (ID I), in the "Seize" cluster, that refers to both building a cybersecurity strategy aligned with the organization's overall strategic plan and guiding its operational declinations (policies, procedures, and attached roles and responsibilities). According to the findings, ID I and ID X should be connected in a closed loop: by continuously evaluating the performance of the implemented strategy, organizations should be able to refine and update their targets, ensuring alignment with the evolving cybersecurity landscape and the organization's goals. ID I also appears to be strictly related to two more capabilities in the "Sense" cluster: ID VI (Identifying and prioritizing cyber risks) and ID XIII (Monitoring 3rd-party cyber risks). Both capabilities are crucial to understand and assess the potential threats and vulnerabilities that an organization may face in the cyber domain. By proactively sensing and seizing opportunities to address these risks, organizations can enhance their cybersecurity posture and mitigate potential harm to their systems, data, and operations.

Table 1. Results of the collection, synthesis and analysis.

ID	Dynamic Capability	N° of Obs.	Cluster	Definition of capability	Goal	References
I	Setting up a comprehensive strategy & governance structure	26	Seize	The capability to set up a well-defined and integrated cybersecurity strategy and governance structure. This capability involves aligning cybersecurity objectives with the overall organizational strategy, establishing related policies and procedures, and defining clear roles and responsibilities.	Ensuring effective guidance and management of the organization cybersecurity efforts.	(Ghaffari & Arabsorkhi, 2019; Kok & Teoh, 2021; Zaini et al., 2020)
II	Building and managing the core cybersecurity architecture	23	Seize	The capability to design, develop, and manage a foundational cybersecurity architecture that encompasses the whole organization infrastructure. This capability involves planning for an integrated security framework, deploying and integrating robust security controls, implementing a wide range of security tools (such as firewalls, intrusion detection and prevention systems, etc.), and maintaining and updating them.	Ensuring overall protection of the organization against cyber threats.	(Dube & Mohanty, 2021; Ghaffari & Arabsorkhi, 2019; Naseer et al., 2018)
III	Fostering the development of cybersecurity skills	22	Transform	The capability to foster a culture of continuous learning and skill development within the organization, with the goal of This capability involves providing training opportunities for employees, fostering a culture of continuous improvement, conducting post-incident reviews and sharing lessons learned, and staying informed about emerging cybersecurity trends.	Adapting employees' skills to evolving challenges, technologies, and best practices.	(Garcia-Perez et al., 2023; Ghaffari & Arabsorkhi, 2019; Naseer et al., 2018)
IV	Enhancing threat prevention	20	Sense	The capability to develop and implement advanced detection systems. This capability involves monitoring continuously all the relevant data sources (e.g., network traffic, system logs), utilizing advanced prevention tools and techniques (such as behavioral analytics, anomaly detection systems, etc.), and integrating and leveraging threat intelligence feeds to identify indicators of compromise and suspicious activities.	Identifying cyber threats to prevent them from compromising the organization.	(Adler, 2013; Ghaffari & Arabsorkhi, 2019; Naseer et al., 2018)
V	Fostering internal and external cybersecurity awareness	19	Seize	The capability to create and promote a culture of cybersecurity, both within the organization and towards its external stakeholders. This capability involves conducting cybersecurity awareness campaigns, communicating regularly about the importance of cybersecurity and the potential risks faced by individuals and the organization as a whole, and encouraging the diffusion of security hygiene practices.	Ensuring security-conscious behaviors across all the organization and its value chain.	(Garcia-Perez et al., 2023; Ghaffari & Arabsorkhi, 2019; Kosutic & Pigni, 2020)
VI	Identifying and prioritizing cyber risks	19	Sense	The capability to assess potential cyber risks and threats. This capability involves setting up a coherent cyber risk appetite for the organization, creating asset inventories, conducting risk assessments, and developing coherent strategies to address the identified risks.	Identifying cyber risks to enable proper mitigation.	(Adler, 2013; Ghaffari & Arabsorkhi, 2019; Kosutic & Pigni, 2020)
VII	Enforcing compliance to laws, regulations, standards	19	Seize	The capability to ensure organizational compliance with relevant laws, regulations, and industry standards pertaining to different aspects of cybersecurity (e.g., product security or data protection). This capability involves identifying, understanding and applying the regulatory requirements, legal frameworks and industry standards that are relevant for the organization.	Ensuring optimization of cybersecurity processes and reduction of legal and regulatory risks.	(Cavusoglu et al., 2015; Podrecca et al., 2022; Dube & Mohanty, 2021)
VIII	Managing incident response	18	Seize	The capability to respond to and recover from cybersecurity incidents in an efficient manner. This capability involves planning for incident response, implementing tools to detect threats, analysing the incidents, containing and eradicating them, and restoring affected systems to their normal operating conditions.	Ensuring minimization of the impact of cybersecurity incidents.	(Adler, 2013; Carcary et al., 2019; Garcia-Perez et al., 2023)
IX	Developing pervasive security operations	16	Transform	The capability to adjust and reorganize business operations to incorporate cybersecurity principles, with the goal of. This capability involves establishing and maintaining pervasive security operations and embedding cybersecurity principles into the development of products, services, and business processes.	Adapting business operations to be secure by design.	(Ghaffari & Arabsorkhi, 2019; Kok & Teoh, 2021; Kosutic & Pigni, 2020)
X	Monitoring and evaluating cybersecurity performances	14	Seize	The capability to continuously assess the effectiveness and efficiency of cybersecurity measures and controls. This capability involves establishing reward structures, performance metrics, and accountability mechanisms that encourage responsible cybersecurity behavior.	Ensuring timely identification of areas for overall cybersecurity improvement.	(Ghaffari & Arabsorkhi, 2019; Kosutic & Pigni, 2020; Naseer et al., 2018)
XI	Selecting and integrating new technologies	13	Sense	The capability to identify, evaluate, and integrate new cybersecurity technologies and solutions into existing systems and processes. This capability involves monitoring technological advancements, conducting technology and vendor assessments, and staying updated on the latest cybersecurity solutions.	Identifying new solutions to provide up-to-date protection against emerging threats.	(Dube & Mohanty, 2021; Holland & Burchell, 2022; Naseer et al., 2018)
XII	Making cybersecurity closer to the users	11	Seize	The capability to design and implement cybersecurity measures in a way that is accessible, user-friendly, and aligned with the needs and abilities of common users. This capability involves considering the needs, knowledge, and behaviors of the common user when developing cybersecurity tools and techniques, presenting them in a user-friendly manner, and providing ongoing feedback and support.	Ensuring full usage of cybersecurity tools and techniques.	(Dube & Mohanty, 2021; Kosutic & Pigni, 2020; Naseer et al., 2018)
XIII	Monitoring 3rd-party cyber risks	10	Sense	The capability to manage cybersecurity risks associated with third-party vendors and service providers. This capability involves establishing cybersecurity requirements for suppliers, ensuring that appropriate security measures and contractual obligations are in place, and conducting continuous assessments throughout the supply chain.	Identifying 3rd-party cyber risks to assure an end-to-end secure ecosystem for the organization.	(Kok & Teoh, 2021; Kosutic & Pigni, 2020; Zaini et al., 2020)
XIV	Integrating cybersecurity and physical security	8	Seize	The capability to integrate physical security measures with cybersecurity. This capability involves analyzing the physical security landscape, developing a security plan that incorporates physical security controls, and combining physical access control with strong authentication mechanisms.	Ensuring security of physical assets, facilities, and infrastructures.	(Carcary et al., 2019; Ghaffari & Arabsorkhi, 2019; Kok & Teoh, 2021)
XV	Collaborating with external entities	7	Sense	The capability to establish and maintain collaborative relationships with external entities. This capability involves participating in initiatives such as information-sharing forums and engaging in collaborative cybersecurity relationships with relevant external stakeholders, such as government entities and regulatory bodies.	Identifying threats outside the view of the organization to expand the overall cybersecurity knowledge.	(Adler, 2013; Garcia-Perez et al., 2023; Kok & Teoh, 2021)
XVI	Implementing security in HR practices	7	Transform	The capability to integrate cybersecurity requirements into human resource management processes. This capability involves implementing robust access controls and privilege management procedures, incorporating security-related clauses into employment contracts and codes of conduct, monitoring compliance with security policies and taking appropriate disciplinary actions for policy violations.	Adapting HR requirements to cultivate a security-conscious workforce.	(Ghaffari & Arabsorkhi, 2019; Kok & Teoh, 2021; Zaini et al., 2020)
XVII	Understanding the cybersecurity needs of customers	5	Transform	The capability to understand and address the security needs and concerns of customers and incorporate their feedbacks and requirements. This capability involves gathering insights from customer expectations (e.g., privacy concerns), developing customer-centric security measures and delivering cybersecurity-compliant products and services.	Adapting products and services to the needs of customers interested in security and privacy features.	(Cavusoglu et al., 2015; Dube & Mohanty, 2021; Kosutic & Pigni, 2020)

ID XIII deserves particular attention considering the several attacks that have recently targeted companies by exploiting vulnerable companies in their supply chain. In this regard, some sources mentioned as key activities to establish long-term relationships with critical vendors and to assess periodically their cyber posture, other than to integrate specific security-related clauses in procurement contracts. Finally, the latest addition to this group of capabilities pertains to the other side of the organization value chain. "Understanding the cybersecurity needs of customers" (ID XVII) seems to be an increasingly relevant capability to establish and preserve their long-term trust, as well as to attract new customers who are interested in these features. The analyzed papers also suggest that being all highly strategic in nature, these five capabilities rely heavily on factors such as the cyber-related knowledge and expertise of the organization's top management, on the business knowledge of its cyber leadership, and on the ability of the cyber leadership to build internal relationships with non-IT units such as procurement and sales.

In the second group, the most mentioned capability is again a "Seize" one, "Building and managing the core cybersecurity architecture" (ID II). ID II was also the capability with the highest number of associated themes. These included several technical and non-technical activities, ranging from the integration cyber with existing IT systems to the deployment of effective security controls, from the monitoring of vulnerabilities and patching of assets to the management of cybersecurity solutions' vendors. ID II underlines the need for an additional capability, ID XI, consisting in the selection of new technologies and tools and ensure that the organization remains up to date with the evolving threat landscape. Additionally, several papers suggest the need for a capability to integrate the core cybersecurity architecture with physical security (ID XIV). This is especially relevant considering the potential synergies between the two (e.g., access monitoring systems that combine "physical" biometric recognition and "digital" data from employee badges) and the fact that certain types of attacks, such as those targeting Operations Technology infrastructures, can lead to cyber-physical consequences. Finally, "Making cybersecurity closer to the users" (ID XII) appears as a necessary capability to ensure full usage of cybersecurity tools deployed as part of the core cybersecurity architecture. What emerges is a significant need to simplify cybersecurity by reducing the tools complexity, providing an intuitive user experience, and offering constant support to end users. Given its nature, the categorization of ID XII as a "Seize" or "Transform" capability, but in this case priority was given to the former, given ID XII's goal of ensuring full usage of the corporate cybersecurity tools and techniques.

A third group of capabilities confirms the importance of training and awareness activities in this context (ID III & ID V). Cybersecurity training and awareness have been a topic of discussion for years because many of the most devastating cyber-attacks originated from simple human mistakes (e.g., ransomware originating from phishing emails). Overall, the analyzed papers suggest that training and awareness activities can be seen as a triad of capabilities aligned with the Sense-Seize-Transform clusters. First, to foster employees' understanding of the current cybersecurity landscape and enable them to identify potential cyber threats, it is essential to have robust awareness and communication capabilities (ID V). Then, employees need to continuously keep learning the necessary skills to respond to such threats (ID III). Finally, recruiting and retention practices need to change to include contractual conditions that require minimum levels of cybersecurity knowledge, participation to cybersecurity training and awareness campaigns, and adherence to cybersecurity policies (ID XVI). As for ID XII, also ID III's categorization is debatable, but in this case priority between "Seize" and "Transform" was attributed to the latter due to ID III's goal of continuously adapting employees' skills to the evolving cybersecurity landscape.

A fourth group of capabilities relates to ensuring business continuity. Capabilities in this group include "Enhancing threat prevention" (ID IV), "Collaborating with external entities" (ID XV), "Managing incident response" (ID VIII) and "Developing pervasive security operations" (ID IX). Similar to the previous one, also this set of capabilities cuts across all three clusters. ID IV, enabled by new technologies and particularly by machine learning analytics, is essential for identifying and preventing several threats that could affect the organization. ID XV can play a pivotal role in strengthening ID IV, by enabling the exchange of knowledge and insights with peer companies and other relevant public entities. This collaborative approach enables the organization to broaden its perspective on the overall cybersecurity environment, gaining valuable contextual information and expanding its threat intelligence range. On the contrary, ID VIII – which again encompasses various technical and non-technical activities, ranging from incident containment and eradication to effective communication with external stakeholders – allows organizations to minimize the impact of all the cyber threats that escaped ID IV and became actual incidents. Lastly, the transformative capability is represented in this case by ID IX, whose purpose is to

embed security by design in products, services, and business processes, thus reducing the organization's attack surface and bolstering the continuity of operations.

Finally, a self-contained capability stands out significantly: "Enforcing compliance to laws, regulations, standards" (ID VII). Although the cybersecurity domain seems to be evolving from a compliance-oriented to a result-oriented approach, the analysis of the papers emphasize that compliance will continue to play a significant role in the success of organizational cybersecurity. This is due to several factors, from the rise of national and international cybersecurity legislations (such as GDPR in Europe and the MLPS scheme in China) to the progressive recognition of international cybersecurity standards like ISO 27001 and NIST CSF, which today are increasingly being used for both internal and external purposes. With the increase of new cybersecurity regulations, laws and standards, it is reasonable to expect that the importance of ID VII will rise considerably over time.

5.2 Comparison with NIST CSF / ISO 27001

The comparison of the identified capabilities with those emphasized by the most applied international frameworks, the NIST CSF and the ISO 27001, unveils some interesting considerations. Firstly, the paper highlights a distinct prevalence of non-technical capabilities over technical ones. Non-technical capabilities like ID I are obviously acknowledged by most cybersecurity frameworks, and yet they often receive less emphasis compared to technical capabilities. This discrepancy is particularly evident in the NIST CSF, where these activities are predominantly addressed only within the "Identify" function. While the NIST CSF does not explicitly state that all five functions have equal importance, their purely numerical representation seems to suggest that "Identify" capabilities have a relatively little weight compared to the others (counting for "only 20%" of the total). On the contrary, a stronger focus is placed on the development and design of the core cybersecurity architecture (most of the Protect activities), and on incident prevention & response (Detect, Respond and Recover functions).

On the contrary, the ISO 27001 clearly points out the importance of strategic aspects, as they constitute the foundation for five out of the eight "clauses" of the framework (Context of the Organization, Leadership, Planning, Performance Evaluation, and Improvement). In contrast, ISO 27001 lacks emphasis on incident prevention & response capabilities, although the controls prescribed by the framework encompass numerous activities related to this domain.

The focus on strategy and organizational skills does not imply that technical aspects of cybersecurity are less important. Capabilities related to the core cybersecurity architecture (ID II, ID XI, ID XII, ID XIV) and capabilities that foster business continuity (ID IV, ID VIII, ID IX and ID XV) – mostly technical in nature – both emerge as crucial for organizations, but they received extensive coverage in both cybersecurity frameworks. However, even in this case, less-technical capabilities such as the "Making cybersecurity closer to the business users" seem to be relatively underestimated.

Regarding training and awareness capabilities (ID III, V, XVI), although their importance is stressed in both frameworks, their overall representation is comparatively less significant than what the findings would suggest (training and awareness are represented in a few activities in the NIST CSF and in the Support clause in the ISO 27001). From this perspective, the role played by Human Resources practices in achieving satisfactory levels of training and awareness seems to be particularly underestimated.

Finally, both frameworks, being focused on cybersecurity as a mean to protect the organization rather than to enhance its competitive advantage, do not address one of the capabilities that emerged from the study: "Understanding the cybersecurity needs of customers".

6. Conclusions and further research

Despite its growing importance, cybersecurity still lacks theoretical studies that provide a holistic understanding of the phenomenon. By systematically categorizing cyber capabilities collected through a rigorous Systematic Literature Review (SLR) and analyzing them within the well-established strategic framework of dynamic capabilities, this study aims to start addressing the existing theoretical gap. The paper specifically identifies 17 cyber capabilities, categorizing them into Sense, Seize and Transform dynamic capabilities in analogy to Teece et al. (1997). Each of the 17 capability is analyzed to understand how it contributes to organizational cybersecurity and how it relates with the others.

While several of these capabilities have been already identified and described in both widely adopted cybersecurity standards (such as ISO 27001 and NIST CSF) and academic and practitioner works (such as Antonucci, 2017; Kosutic & Pigni, 2020), the findings of the paper emphasize the important role played by non-technical capabilities vs. technical ones. The paper also proposes a different

categorization of cyber capabilities, departing from the typical NIST CSF or ISO 27001 approaches and organizing the findings based on a more strategic-oriented framework such as the dynamic capabilities one. Finally, the paper highlights the relevance of capabilities that have been partially or totally overlooked by today's frameworks, namely "Making cybersecurity closer to the users", "Implementing security in HR practices" and "Understanding the cybersecurity needs of customers".

This work serves as the initial step in a research direction that could provide numerous insights for future studies. For instance, within the realm of dynamic capabilities, the paper primarily considers the definition offered by Teece et al. (1997) rather than equally relevant interpretations like that provided by Eisenhardt & Martin (2000). According to Peteraf et al. (2013), the two interpretations represent *"not only different but contradictory understandings of the construct's core element".* Further research could investigate whether dynamic capabilities align more closely with the former or the latter interpretation. In a similar vein, forthcoming works could elaborate if a hierarchy of higher-order cyber capabilities exists (Peteraf & Barney, 2003; Winter, 2003), and determine which ones exhibit Valuable, Rare, Imperfectly Imitable and Non-substitutable (VRIN) traits (Peteraf et al., 2013). Another research stream could investigate the antecedents that enable these dynamic capabilities or the microfoundations that they are based upon. Microfoundations refer to the underlying individual-level attributes, skills, and capabilities that contribute to the development and execution of organizational capabilities (Teece, 2007). The literature examined in this paper frequently highlights corporate culture and the Board's knowledge of cybersecurity as crucial factors for achieving dynamic capabilities in the cyber domain. On the other side, certain microfoundations might be associated with the competencies exhibited by senior cyber leadership, particularly by the CISO. Lastly, it is realistic to imagine that dynamic cyber capabilities will evolve over time: therefore, it is reasonable to assume that certain cyber capabilities highlighted in this paper will become less or more relevant in the future. In this sense, this work should be interpreted as a snapshot of the current state of cybersecurity, serving as a starting point for future works that address new capabilities of particular relevance to organizations.

7. References

Abbatemarco, N., Gaur, A., & Meregalli, S. (2022). Stuck in Pilot Purgatory: Understanding and Addressing the Current Challenges of Industrial IoT in Manufacturing. *Proceedings of the 55th Hawaii International Conference on System Sciences*.

Adler, R. M. (2013). A dynamic capability maturity model for improving cyber security. Proceedings of the *2013 IEEE International Conference on Technologies for Homeland Security (HST)*, 230–235.

Almuhammadi, S., & Alsaleh, M. (2017). Information Security Maturity Model for Nist Cyber Security Framework. *Computer Science & Information Technology*, 51–62.

Antonucci, D. (2017). *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*. John Wiley & Sons.

Barrett, M. (2018). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework*.

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. *Journal of Systems and Software*, *80*(4), 571–583.

Carcary, M., Doherty, E., & Conway, G. (2019). A capability approach to managing organisational information security. *Proceedings of the 2019 European Conference on Information Warfare and Security.*

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., & Benbasat, I. (2015). Institutional pressures in security management. *Information and Management*, *52*(4), 385–400.

Chhetri, S. R., Faezi, S., Rashid, N., & Al Faruque, M. A. (2018). Manufacturing Supply Chain and Product Lifecycle Security in the Era of Industry 4.0. *Journal of Hardware and Systems Security*, *2*(1), 51–68.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21.

Donaldson, S., Siegel, S., Williams, C. K., & Aslam, A. (2015). *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats*. Apress.

Dube, D. P., & Mohanty, R. P. (2021). The application of cyber security capability maturity model to identify the impact of internal efficiency factors on the external effectiveness of cyber security. *International Journal of Business Information Systems*, *38*(3), 367–392.

Eisenhardt, K. M., & Martin, J. A. (2000). Dynamic capabilities: What are they? *Strategic Management Journal*, *21*(10–11), 1105–1121.

Garcia-Perez, A., Sallos, M. P., & Tiwasing, P. (2023). Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: An intellectual capital perspective. *Journal of Intellectual Capital*, *24*(2), 465–486.

Ghaffari, F., & Arabsorkhi, A. (2019). A New Adaptive Cyber-security Capability Maturity Model. *Proceedings of the 9th International Symposium on Telecommunications (IST).*

He, W., & Zhang, Z. (Justin). (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, *29*(4), 249–257.

Helfat, C. E., & Peteraf, M. A. (2009). Understanding dynamic capabilities: progress along a developmental path. *Strategic organization*, 7(1), 91–102.

Holland, M. C., & Burchell, J. (2022). Low Resource Availability and the Small- to Medium-sized Retail Enterprise's Ability

to Implement an Information Security Strategy. *Business Management Research and Applications*, *1*(2), 48–76.

ISO. (2022). *ISO/IEC 27001*.

Jacobs, P., von Solms, S., & Grobler, M. (2016). Towards a framework for the development of business cybersecurity capabilities. *Proceedings of the International Conference on Business and Cyber Security (ICBCS)*, *7*(4), 51–61.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993.

Kitchenham, B., & Charters, S. (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering. *Technical Report EBSE 2007-001, Keele University and Durham University Joint Report*.

Kosutic, D., & Pigni, F. (2020). Cybersecurity: Investing for competitive outcomes. *Journal of Business Strategy*, *43*(1), 28–36.

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248.

Leonardi, P. M. (2021). COVID-19 and the New Technologies of Organizing: Digital Exhaust, Digital Footprints, and Artificial Intelligence in the Wake of Remote Work. *Journal of Management Studies*, *58*(1), 249–253.

Levy, Y., & Gafni, R. (2021). Introducing the concept of cybersecurity footprint. *Information & Computer Security*, *29*(5), 724-736.

Madnick, B., Huang, K., & Madnick, S. (2023). The evolution of global cybersecurity norms in the digital age. *Information Security Journal: A Global Perspective*, *0*, 1–22.

Mikalef, P., Pappas, I. O., Krogstie, J., & Giannakos, M. (2018). Big data analytics capabilities: A systematic literature review and research agenda. *Information Systems and E-Business Management*, *16*(3), 547–578.

Morgan, S. (2018, February 27). Global Ransomware Damage Costs Predicted To Exceed $5 Billion In 2017. *Cybersecurity Ventures*. Retrieved on Jun 6th, 2023 from: https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/

Naseer, H., Maynard, S. B., Ahmad, A., & Shanks, G. (2018). Cybersecurity risk management using analytics: A dynamic capabilities approach. *Proceedings of the 2018 International Conference on Information Systems.*

Pala, A., & Zhuang, J. (2019). Information Sharing in Cybersecurity. *Decision Analysis*, *16*(3), 172–196.

Peppard, J., & Ward, J. (2016). *The Strategic Management of Information Systems: Building a Digital Strategy*.

Peteraf, M. A., & Barney, J. B. (2003). Unraveling the resource-based tangle. *Managerial and Decision Economics*, *24*(4), 309–323.

Peteraf, M., Di Stefano, G., & Verona, G. (2013). The elephant in the room of dynamic capabilities: Bringing two diverging conversations together. *Strategic Management Journal*, *34*(12), 1389–1410.

Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*, *142*, 103744.

Rothrock, R. A., Kaplan, J., & van Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review*, *59*, 12–15.

Sabillon, R., Cano M., J., Serra-Ruiz, J., & Cavaller, V. (2016). Cybercrime and Cybercriminals: A Comprehensive Study. *International Journal of Computer Networks and Communications Security*, *4*, 165-176.

Salviotti, G., Abbatemarco, N., De Rossi, L. M., & Bjoernland, K. (2023). Understanding the Role of Leadership Competencies in Cyber Crisis Management: A Case Study. *Proceedings of the 56th Hawaii International Conference on System Sciences*.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *The Journal of Digital Forensics, Security and Law*, *12* (2), 53–74.

Scofield, M. (2016). Benefiting from the NIST CSF. *Information Management Journal*, *50*(2), 25–29.

Sen, R. (2018). Challenges to Cybersecurity: Current State of Affairs. *Communications of the Association for Information Systems*, *43*(1).

Sharkov, G. (2016). From Cybersecurity to Collaborative Resiliency. *Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense*, 3–9.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security. *Future Generation Computer Systems*, *92*, 178–188.

Stouffer, K., Zimmerman, T., Tang, C., Pease, M., Cichonski, J., Shah, N., & Downard, W. (2019). *NISTIR 8183A Vol. 1*. National Institute of Standards and Technology.

Suryotrisongko, H., & Musashi, Y. (2019). Review of Cybersecurity Research Topics, Taxonomy and Challenges. Proceedings of the *IEEE 12th Conference on Service-Oriented Computing and Applications*.

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*, *28*(13), 1319–1350.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, *18*(7), 509–533.

Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC Medical Research Methodology*, *8*(1), 45.

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. *British Journal of Management*, *14*(3), 207–222.

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102.

Weil, T., & Murugesan, S. (2020). IT Risk and Resilience—Cybersecurity Response to COVID-19. *IT Professional*, *22*(3), 4–10.

Willard, G. (2015). Understanding the Co-Evolution of Cyber Defenses and Attacks to Achieve Enhanced Cybersecurity. *Journal of Information Warfare*, *14*(2), 16–30.

Winter, S. G. (2003). Understanding dynamic capabilities. *Strategic Management Journal*, *24*(10), 991–995.

Xiao, Y., & Watson, M. (2019). Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research*, *39*(1), 93–112.