Communications of the Association for Information Systems

Volume 53 Paper in press

2023

Dynamic Capabilities in Cybersecurity Intelligence: A Meta-Synthesis to Enhance Protection Against Cyber Threats

Angélica Pigola
University Nove de Julho, a_pigola@uni9.edu.br

Priscila Rezende da Costa
University Nove de Julho

Communications of the Association for Information Systems

Accepted Manuscript

Dynamic Capabilities in Cybersecurity Intelligence: A Meta-Synthesis to Enhance Protection Against Cyber Threats

Angélica Pigola
University Nove de Julho
São Paulo, Brazil
a_pigola@uni9.edu.br
0000-0002-7222-5589

Priscila Rezende da Costa
University Nove de Julho
São Paulo, Brazil
0000-0002-7012-0679

Please cite this article as: Pigola, A., & da Costa, P. R. (in press). Dynamic Capabilities in Cybersecurity Intelligence: A Meta-Synthesis to Enhance Protection Against Cyber Threats. *Communications of the Association for Information Systems.*

Communications of the Association for Information Systems

Research Paper ISSN: 1529-3181

Dynamic Capabilities in Cybersecurity Intelligence: A Meta-Synthesis to Enhance Protection Against Cyber Threats

Angélica Pigola
University Nove de Julho
São Paulo, Brazil
a_pigola@uni9.edu.br
0000-0002-7222-5589

Priscila Rezende da Costa
University Nove de Julho
São Paulo, Brazil
0000-0002-7012-0679

Abstract:

Advanced cybersecurity threats with automated capabilities are on the rise in industries such as finance, healthcare, technology, retail, telecoms, and transportation, as well as government. It is necessary to conduct analyses of cybersecurity-related resources and capabilities to build cybersecurity intelligence (CI). In this paper, the purpose is to suggest a dynamic capability in cybersecurity intelligence (DCCI) model based on existing literature that helped firms to reduce risks of cyber violations and advance the development of systems and the life cycle of firms. Through a meta-synthesis, an abduction and induction approach through eight methodological steps analyzed in forty-seven case studies the presence of cybersecurity capabilities to build CI. Combining theoretical and practical information security maturity models as foundation, we understand capabilities building to improve the predictability of cyber incidents. The results evidenced four second-order dimensions to build CI named doing, enabling, improving, and managing cybersecurity and eight first-order outcomes to represent the DCCI model. This research makes an unprecedented contribution to international and national scenarios, as it will allow firms to innovate their resource management processes and abilities to enable better cybersecurity projects and reduce the impacts of potential cyberattacks, with the probability of eradicating vulnerabilities.

Keywords: Cybersecurity, Dynamic Capabilities, Capability Maturity, Meta-Synthesis, Cybersecurity Intelligence.

[Department statements, if appropriate, will be added by the editors. Teaching cases and panel reports will have a statement, which is also added by the editors.]

[Note: this page has no footnotes.]

This manuscript underwent [editorial/peer] review. It was received xx/xx/20xx and was with the authors for XX months for XX revisions. [firstname lastname] served as Associate Editor.] **or** The Associate Editor chose to remain anonymous.]

1 Introduction

Cyberattacks pose an ongoing threat as they are increasingly sophisticated, and companies seek to develop and implement innovative technologies that inadvertently require new and subtle capabilities for developers. A decade ago, cybersecurity was a matter of "if" a company would be affected or compromised, but nowadays it's a matter of "when" and "at what level" (D'Arcy et al., 2020; Jalali et al., 2019; Kour & Karim, 2020). The aftermath of recent critical cyberattacks has affected many firms and many of them did not have appropriate cybersecurity intelligence to handle them. For example, in 2020, hackers leaked information on login credentials of members of staff of the World Health Organization. In 2021, a series of cyberattacks affected at least 10 Sri Lankan National Websites including the Google.lk domain, and JBS S.A., a Brazil-based meat processing company, disabling its beef and pork slaughterhouses, which impacted facilities in the United States, Canada, and Australia. In 2022, the International Committee of the Red Cross made a public plea to hackers who had attacked the organization. All these events among others revealed how relevant it is for firms to remain vigilant to protect themselves from cyber incidents. Furthermore, the presence of a high level of system security failures was recently associated with breach costs that were $2.30 million higher than breach costs at firms without this factor (IBM Security, 2021). Beyond financial impact (Cavusoglu et al., 2004), a cybersecurity weaknesses may cause irreparable harm to a company in the form of corporate liability (Chellappa & Pavlou, 2002), and a weakened competitive position due to loss of credibility (Crossler et al., 2013; Jalali & Kaiser, 2018).

Therefore, firms must improve their approach to developing cybersecurity capabilities aimed at achieving cybersecurity intelligence for their protection. Recently, Kolini and Janczewski (2022) introduced a framework for cybersecurity intelligence to develop a broader information security awareness to respond quickly to large-scale cyberattacks to protect critical assets. The authors mentioned that 'cybersecurity intelligence provides knowledge of attacker's capabilities, motives, resources, and objectives to assist firms in their decision-making processes enhancing their defense strategies.' [(Kolini & Janczewski, 2022) p. 93]. The relevance of being prepared and proactively engaged in building cybersecurity capabilities is more cost-effective than taking a reactive approach in cybersecurity (Adams & Makramalla, 2015; Benz & Chatterjee, 2020; Kwon & Johnson, 2014). While many firms are already aware of the importance of cybersecurity, a large number of firms remain out of date on the main cybersecurity capabilities and technological requirements for cyber protection (Benz & Chatterjee, 2020; Kabanda et al., 2018).

Considering this business scenario supported by a continuous improvement in the cybersecurity posture through capability maturity models that help to achieve this purpose (Dube & Mohanty, 2020), we investigated under the perspective of dynamic capabilities theory the presence of technological, organizational, and managerial capabilities in the literature that have been shaped to build cybersecurity intelligence. Many authors (Dube & Mohanty, 2020; Ghaffari & Arabsorkhi, 2018; Rea-Guaman et al., 2017) investigated and compared several cybersecurity capabilities maturity models and standards resolving specific threats exist. Adler (2013) was one of the first extended cybersecurity capability model into a dynamic performance management framework through an intuitive model-simulate-analyze methodology. Other authors (Akinsanya et al., 2019) presented a literature review of cybersecurity maturity models for cloud security assessment in healthcare and mentioned that there is a lack of organized maturity models available. In this vein, this meta synthesis intend to deliver a dynamic capability in cybersecurity intelligence (DCCI) model based on existing literature. The research question posited is:

RQ1. What are these dynamic capabilities that build firms' cybersecurity intelligence?

This approach is valuable for firms' change and performance against cybersecurity weaknesses. We provide the DCCI model investigating evidences of dynamic capabilities in 47 cases studies as of theoretical evidence from the Capability Maturity Model Integration (CMMI Institute, 2019) that enables firms to build, assess, and improve their processes and capabilities in cybersecurity and the Building Security in Maturity Model (BSIMM, 2022) that quantified the security practices of many firms through a total of one hundred and nineteen activities in information security. This investigation has never been done before, and the DCCI model is closer to a realist approach from this sample of findings through meta-synthesis method. In other words, the purpose of this paper is to present a representation of technological, organizational, and managerial capabilities in cybersecurity to build firms' cybersecurity intelligence evidenced in real case studies. In an organized way, we also considered a progressive

perspective from the dynamic capabilities (DCs) theory. As firms' proactive and reactive decisions in developing cybersecurity dynamic capabilities have received little attention - especially regarding to cyber risks uncertainties and misconceptions about delays in realizing the benefits of these capabilities (Catota et al., 2019; Dhillon et al., 2021) – the findings reveal evidence in four second-order capabilities dimensions and eight first-order capabilities outcomes to represent the DCCI model and support firms in decision-making on cybersecurity building capabilities.

Nevertheless, while there is a wide range of biases in firms' standpoints regarding dynamic capabilities in cybersecurity (Jalali et al., 2019; Rodgers et al., 2020; Rosoff et al., 2013), this paper also tries to contribute to theory and practice. It contributes to introduce the perspective of cybersecurity in DC theory, and add the dynamic perspective of capabilities to information systems (IS) research by: (a) highlighting the main dimensions and outcomes of DCCI to build cybersecurity intelligence; (b) theorizing about the representativeness of the main capabilities to be considered as DCCI; (c) pointing out the impact of DCCI in real case study scenarios regarding the development of virtual protection and organizational change and performance in cybersecurity; and (d) presenting an innovative perspective for the cybersecurity intelligence index developed for firms. This research theorizes about the research field following on to the building sections of meta-synthesis, ending with the conclusion section pointing out its limitations, theoretical and practical contributions, and suggestions for future research.

2 Theoretical Positioning

According to some authors (Goode & Lacey, 2021; Leukfeldt et al., 2017; Spicer, 2019), cybercriminals and system hackers may possess a different way of viewing the world, thereby giving them alternate capabilities in this context. Thus, to research in the field of cybersecurity “it is not enough to approach things in a logical and critical capacity, but one has to be willing to think unorthodoxly” (Steinmetz, 2015 p.131). Therefore, this paper assumes the theoretical lens of dynamic capabilities (DC) to build a capabilities model to provide microfoundations and understand under a range of abilities and process on how firms may enhance cybersecurity intelligence to change and performance in a certain field of business (Eisenhardt & Martin, 2000; Teece, 2007).

A cybersecurity posture may be considered a dynamic and non-negotiable requirement of being in business which demands a continuous improvement in technologies and capabilities to manage cyber-threats (Dube & Mohanty, 2020). Thus, capabilities guidelines are mainstream to information security management serving as continuous measurement of improvement for technologies and cybersecurity posture on an ongoing basis. The research work of capabilities maturity models in information systems started with the formulation systems security engineering capability maturity model (SSE-CMM), afterwards the information security maturity model (ISMM), the NIST cybersecurity framework (Ngwum, 2016; Sedgewick, 2014), and more recently the cyber security capability maturity model (CSCMM) (Dube & Mohanty, 2020), among others. However, they have been subject to criticism because lack an empirical foundation, oversimplify business reality, and do not demonstrate their purpose and managerial implications (Becker et al., 2009, 2010; Dube & Mohanty, 2020; McCormack et al., 2009).

Additionally, the idea of capability maturity models in cybersecurity emerged from the fact that information security management is the result of a bunch of activities managed dynamically, not in isolation (Stevanovic, 2011). Hence, considering the dynamic threat scenario, the over increasing compliance requirement, and the trust in information systems, the arguments of some authors (Akinsanya et al., 2019; Dube & Mohanty, 2020) that it is always necessary additional capabilities models to prescribe the to-be requirements to enhance cybersecurity posture and conduct an as-is analysis on a periodic interval to understand the updates, an important perspective for theoretical and practical advancement. For this challenge, the dynamic capabilities theory (Eisenhardt & Martin, 2000), may serve a impactful support because it posits capabilities as a set of specific and identifiable abilities and processes to manage resources.

Building upon the Resource Based View theory (Barney et al., 1987), DC’s microfoundations aim at high-velocity markets, pointing out that DCs rely on new knowledge created for a specific context. Furthermore, it highlights that routines are purposefully simple, iterative, and cognitively mindful, not linear, and mindless, to allow for emergent adaptation, although not completely unstructured (Eisenhardt & Martin, 2000). Thus, our DCCI framework emerges from a strong learning process about unorthodox ways of thinking (viewing) about the world translated into algorithms, systems architectures, technological process and routines to enhance cybersecurity intelligence (Goode & Cruise, 2006; Wolfe & Hermanson, 2004).

The DCCI model was built to be a representation of dynamic capabilities to enhance cybersecurity intelligence and not to be a maturity model. Despite we applied a structure of capabilities emerged from two maturity models, as explained in the next section, they were reference of identifying technological, organizational, and managerial capabilities considered relevant to build cybersecurity intelligence in the case studies. Finally, it emerges from empirical evidence, also known as sensory experience, it is the knowledge received by observation and experimentation of real cases about their cybersecurity posture. This validation thus gives a scientific footing to the model and hence become more acceptable and implementable (Dube & Mohanty, 2020).

3 Theorizing to Build Dynamic Capabilities in Cybersecurity Intelligence Framework

To build theoretical foundations, it is crucial to understand DCs in IS research. Seminal definitions of DCs underline their nature as an ability (Helfat et al., 2009; Teece et al., 1997; Zahra et al., 2006), whereas others denote them as processes that are identifiable, stable, or repeatable and routines (Eisenhardt & Martin, 2000; Zollo & Winter, 2002). Recently, Steininger et al. (2022) presented in a literature review the Nomological Net of Dynamic Capabilities, developing an organizing framework that involves organizational change outcomes, the enabling resources, the effects of the external environment, the organizational performance outcomes, and the role of business strategy. Additionally, the authors highlighted a distinction between the first-order outcomes, which concern the organizational change in which DCs result, including new or modified ways of operating, and the second-order outcomes, which reflect organizational performance effects that are a result of the organizational change created by DCs (Steininger et al., 2022).

Traditionally, IS research identify resources as embracing both capabilities and assets (Piccoli & Ives, 2005), with assets being "anything intangible and tangible applied in firms' processes for creating, offering or producing in services or products" (Wade & Hulland, 2004, p. 109), whereas capabilities are “a firm’s capacity to deploy [assets,] … in combination [with other] organizational processes, to effect a desired end” [(Amit & Schoemaker, 1993) p. 35; quote adapted based on (Steininger et al., 2022; Wade & Hulland, 2004)]. Steininger et al. (2022) classified resources as technological, organizational and as well as managerial ones. Technological resources are associated with IT capabilities allowing firms to analyze and make sense of their challenging environments with more accuracy and speed to capitalize on emerging opportunities. Studies have shown that IT capabilities are of higher value under conditions of high informational complexity (Mikalef et al., 2021) and in fast-paced environments (Lee et al., 2015; Pavlou & El Sawy, 2006). Organizational and managerial resources, together, are concerned with how processes and decision-making influence DCs. The motivation for incorporating such aspects lies in the theorized synergies for shaping DCs (Hock-Doepgen et al., 2021; Steininger et al., 2022). Organizational externalities are viewed as mechanisms to expand boundaries of rationality and facilitate evolutionary organizational fitness (Helfat & Winter, 2011) and IT capabilities complement these organizational approaches by serving as the vehicle on which such evolution can be enacted (Iyengar et al., 2015).

Providing a comprehensive, consistent, and pragmatic understanding of the multifaceted construct of DCs, Steininger et al. (2022) understand DCs as "encompassing (1) sensing or the capacity to scan the environment, to spot new developments, and to identify both opportunities and threats; (2) seizing or the capacity to act upon newly sensed opportunities by making decisions; and (3) transforming or the capacity to change (i.e., acquire, recombine, eliminate) resources in relation to the pursued identified opportunities”. The three attributes purposely exclude both the causes and effects of DCs in order to avoid tautologies (Barreto, 2010; Burisch & Wohlgemuth, 2016; Laaksonen & Peltoniemi, 2018; Steininger et al., 2022). However, from a cybersecurity intelligence perspective, it is relevant to shape the understanding of the phenomena. Following Kolini and Janczewski (2022), we define cybersecurity intelligence as dynamic processes and abilities to identify the knowledge of attacker's capabilities, motives, resources, and objectives to assist firms in their decision-making processes enhancing their defense strategies (Kolini & Janczewski, 2022).

To organize the perspective of DCCI, we first took from the literature the Capability Maturity Model Integration (CMMI Institute, 2019) that offers a proven collection of global best practices to help firm to develop and benchmark their capabilities. The structure of CMMI consists of four main categories (Doyle, 2018): (1) Doing, to develop quality products; (2) Enabling, to support the development of products; (3) Improving, for performance; and (4) Managing, for the development of products (Al-Matouq et al., 2020;

CMMI Institute, 2019). CMMI is the most widely used model in the software industry (Al-Matouq et al., 2020). It enables firms to build, assess, and improve their processes and capabilities (CMMI Institute, 2019).

Second, we identified from the Building Security in Maturity Model (BSIMM, 2022) the nineteen activities developed by a team of leading software security experts in 2008 who quantify the security practices of many firms providing common ground that enable a comparison of security initiatives. Al-Matouq et al., (2020) summarized and developed from BSIMM, a security software design maturity model, evaluating it in different software firms and highlighting that the model improves firms' software design security through seventy-one best practices that also offer a foundation for researchers to develop new software security propositions.

Finally, we built the DCCI model through analyzing the seventy-one cybersecurity practices identified by Al-Matouq (2020) and dimensions from capability maturity model integration (CMMI Institute, 2019), bringing in the perspective of DCs presented by (Steininger et al., 2022), to theorize about DCCI, looking for the level of process and abilities that build effectiveness in the management and commitment of firms to implement innovations, promote change and pursue performance in cybersecurity. These references were used to search for and measure its consistency and coverage, together with the breadth of its results across each analyzed case study. We sought evidence of these practices and capabilities to build our DCCI framework. The summary of BSIMM, CMMI and DCs microfoundations served as guidelines to find capabilities throughout the forty-seven case studies.

The dimensions consist of four main categories, namely Doing, Managing, Enabling, and Improving, and each of them has one or more groups of practices called knowledge areas (CMMI Institute, 2019). The described best practices assess the organization's capabilities against enhancing key capabilities (technological, managerial, and organizational), process improvements and abilities to provide evidence of successful cybersecurity achievement to satisfy business requirements (Al-Matouq et al., 2020). These practices are organized into eight categories that have a nature of outcomes. To classify this nature, we looked at the practices through the DCs perspective as an ability (Helfat et al., 2009; Teece, 2007; Teece et al., 1997), or as processes that are more or less identifiable, repeatable, stable, or routine (Eisenhardt & Martin, 2000; Zollo & Winter, 2002). In the end, identifying the sources of where practices emerge or come from (processes or abilities), made it possible to identify the resources that they involve (assets or capabilities) and the outcomes that they generate both organizational change and performance in cybersecurity (Piccoli & Ives, 2005; Steininger et al., 2022).

4 Meta-Synthesis Methodological Design

As meta-synthesis requires attention in both evidence analysis across the studies as well as ensuring sensitivity regarding contextualities, a research protocol suggested by Hoon (2013) was followed about how to build theory via synthesizing case studies. A meta-synthesis protocol is suitable for substantiating the certain path and logic of the method, thereby enhancing its reliability (Pratt, 2008). Meta-synthesis relies on an additive model of evidence while minimizing contextual differences, offering a general line of inquiry to explore the existing variation of relations across the studies being treated as intervening variables (Aguinis et al., 2011; Cortina, 2003; Dalton & Dalton, 2008; Hoon, 2013; Kisamore & Brannick, 2008; Rousseau et al., 2008). Meta-analyst scholars have generated transparent rules on how to report on the conduct of meta-analysis with replicability being classified as enhancing the product of a synthesis (Aytug et al., 2012; Carlson & Ji, 2011; Dalton & Dalton, 2008; Hoon, 2013).

All the steps involved in this meta-synthesis are in the following sections. A description of the procedures and actions applied as well as their purpose are shown in Table 1. The research approach focuses on capabilities in cybersecurity, specifically those considered DCs. Even in the body of literature providing interpretations of technological, organizational, and managerial capabilities in cybersecurity, those considered as DCs have not been sufficiently evidenced (Steininger et al., 2022).

Table 1. Meta-Synthesis Protocol

Steps in Meta-Synthesis	Analytical Description	Analytical Procedure	Outcome of each step
Framing research question (Section 4.1)	Conceptually embedding the meta-synthesis in the field of research technological, organizational, and managerial cybersecurity capabilities; identifying a clear research question addressing the capabilities with characteristics as DCs in changing, performing, or innovating in cybersecurity.	A priori specification	Identification of a well-specified research question to validate variables accurately and extracting appropriate data from primary technological, organizational, and managerial capabilities studies in cybersecurity.
Locating relevant research (Section 4.2)	Identifying the body of research in cybersecurity capabilities (technological, organizational, and managerial) that is relevant for the research question of interest. Following an exhaustive literature search to prevent the exclusion of relevant information, thus strengthening the findings from a broader base.	Determining the keywords; search string validated by specialists; an exhaustive search strategy formulated entailing main and complementary search steps	Locating a sample of 438 publications on cybersecurity capabilities and selecting eighty-one relevant IS journals. A screening of papers with the methodological approach - case studies – generated the final sample of eighty-nine papers.
Inclusion criteria (Section 4.3)	Precise inclusion and exclusion criteria were applied to select only case studies that explicitly addressed the cybersecurity capabilities approach to determine which studies to include	Developing and discussing an inclusion/exclusion precise criteria list.	Limiting eighty-nine case studies to a set of forty-seven cases which finally incorporated a cybersecurity capabilities approach, the meta-synthesis analysis provided clear exclusion criteria to ensure validity, reliability, replicability of the method.
Coding data (Section 4.4)	Carefully read the full text of each case study. Coding characteristics as well as the proceeded insights of the primary studies in accordance with the research question on cybersecurity capabilities as DCs.	Developing and pretesting a coding form and checking for intercoder ratings.	Code, categorize and order evidence from each of the studies considering contexts-specific, validating coding form and codification ratings
Analyzing on a paper-specific level (Section 4.5)	Identifying a sequencing of variables in each case study to be the most influential in accounting for how capabilities change and perform in cybersecurity as DCs.	Paper-specific causal	Identifying themes, patterns, core concepts and relationships in each case study
Synthesizing across paper level (Section 4.6)	Merging the paper-specific into a meta-causal network. Concentrating the sequencing of variables at a cross-paper level to find out a standard among the variables.	Meta-network, variable ratings	Identification of a pattern; DCCI as central variables; rating of the variables to assure consistency of findings.
Results of DCCI model (Section 5)	Identification of the concept of DCs that explains interdependencies among cybersecurity capabilities representations, adjustments and renewal in environments characterized by uncertainties and changes, demonstrating a significant contribution	Linking the results back to the literature on DCs	Clarification of the second-order dimensions of DCCI; arguing for their contribution to practice and theory
Discussion with specialists (Section 6)	Discussion of the results with specialists, methodological checking, and potential limitation	Discussing credibility, transferability, dependability, and confirmability	Legitimizing credibility, transferability, dependability and confirmability of the procedures and activities used with specialists

Adapted from Hoon (2013)

4.1 Framing the Research Question

Starting with a conceptual framing of the topic (step 1), it consisted of studying the existing literature on capabilities in cybersecurity and DCs for the identification of the problem or phenomenon. To organize the meta-synthesis, interesting recent studies on capabilities with a specific approach to cybersecurity intelligence were targeted. Within this view, organizational, managerial and technological capabilities have been a critical element in activities of cybersecurity intelligence, with some of them considered as DCs to achieve sustained competitiveness through more predictability with regard to uncertainties (Gërguri-Rashiti et al., 2017; Valdez-Juárez & Castillo-Vergara, 2020; Zahra et al., 2006). Therefore, the first broad research topic is related to the role of technological, organizational, and managerial capabilities in the development of DCCI. Addressing the research question aids the current knowledge of practitioners and scholars in interpreting and acting on DCs, thereby offering managerial and theoretical insights into the development of DCCI in highly contested unpredictable environments. This iterative process of framing research question was conducted by the authors and two additional specialists in cybersecurity.

A meta-synthesis takes advantage of a well-specified, theoretically informed research question, in contrast to the broader research interests of a conventional literature review or a systematic review (Aguinis et al., 2021; Hoon, 2013; Paré et al., 2015; Snyder, 2019). Additionally, the more fine-grained and narrow the research question, the greater the conceptual clarity and interpretability of the results (Yin, 2014). Therefore, this well-specific research question shepherded the range of studies that were synthesized and enabled the extraction of appropriate evidence from the primary studies. However, any advantage gained from the interpretability of empirical results is offset by considerations of the availability of evidence for the meta-synthesis (Hoon, 2013). In this paper, the research question proved to be broad enough to open an important set of high-quality studies, while its narrowness enabled the identification of a set of studies that corresponded to the topic of interest.

4.2 Locating Relevant Research

In this step (step 2), the body of research deemed relevant for the meta-synthesis was identified. To locate the set of existing case studies, the approach adopted in the search query considered recommendations of Tran et al. (2022) about how good search strings are. The authors mentioned that a search string can be done manually identifying relevant venues (conferences, workshops, and journals) and researchers; or informally searching an electronic data sources; or using expert's recommendations; or using an existing search string to save time and efforts (Tran et al., 2022). In this vein, to solve issue related to avoid using generic search terms, search filters that could neglected important publications and the search repeatability in terms of impossibilities of replication the search result, we decided to combine two approaches one using partially the search string applied in Dhillon et al. (2021), and other using two expert's recommendations adopting different strategies for each database of choice.

Data was retrieved from two main repositories that are commonly used by researchers in information systems, Clarivate Analytics' Web of Science (WoS) and Association for Information Systems (AIS) Journals at AIS Electronic Library (AISeL). WoS database was chosen because it is estimated to be one of the main interdisciplinary databases of the highest quality standard and one of most reliable (Akbari et al., 2021; Merigó et al., 2015). In turn, AISeL indexes more than 58,354 active records in information systems including peer-reviewed journals, books, and conference proceedings. The search on the WoS was operationalized with an initial search based on the search string as follow:

security OR privacy* OR cyberaggresive OR cybercrime OR cyberdeviance OR cyberinsurance OR cyberloafing OR cyberstalking OR cyberrisk* OR confidentiality OR hacking OR firewall OR "access control" OR phishing AND capabilit* AND organization* OR firm* OR business* OR enterpris* AND case stud**

Additionally, the search on the AISeL were also operationalized with an initial search based on the following search string:

"*cybersecurity" AND "capabilities" OR "dynamic capabilities"*

These keywords were used as a selection criterion for topic (title, keyword, abstract) without time limit, resulting in an initial sample of 438 publications, after excluding repeated publications within the databases. In addition, following methodological recommendations and statements provided by (Aguinis et al., 2020) related to journals ranked by the Journal Citation Reports (JCR 2021), we categorize a list of main journals selected in the IS research field. The list of journals is provided in Appendix A. Proceedings,

editorials, and books were excluded considering only papers published in the selected journals which receiving a cross-checking of methodological approach to identify the sample of eighty-nine case studies published between January 1995 and March 2022 and where the abstracts and keywords varied in content.

After reading, analyzing, and applying this first stage of inclusion and exclusion criteria previously defined, we presented in the next section the second stage of inclusion and exclusion criteria showing the content of each paper. We searched for references to capabilities in cybersecurity, and the overall full-text search generated a list of forty-seven case studies referring directly to capabilities in cybersecurity research field. In sum, any synthesis should be exhaustive in its inclusion of studies by selecting the maximum number of eligible primary sources (Aytug et al., 2012; Hoon, 2013; Kisamore & Brannick, 2008). Furthermore, a systematic, explicit, and transparent search process generates a rigorous meta-synthesis, thereby acknowledging that ill-defined or biased searches are likely to result in an inadequate database and later, inaccurate results (Aytug et al., 2012; Cooper, 2017; Hoon, 2013).

Hoon (2013) highlighted that "relying on published literature is not without risk since only a comprehensive search is associated with limiting the potential of publication bias" and the benefits of published papers entail the increased scientific rigor resulting from a peer-reviewed publication process. More critically, the author pointed out case studies as being less likely or even more difficult to publish, especially in top-tier journals. Hence, the search strategy of papers published in high-quality journals, excluding papers published in conference proceedings, and book chapters, as well as dissertations and unsubmitted or unpublished research studies.

4.3 Inclusion and Exclusion Criteria

Determining and adopting the inclusion/exclusion criteria (step 3) is a central basis of meta-synthesis because its validity depends on the quality of the primary studies (Dalton & Dalton, 2008; Hoon, 2013). Drawing upon the defined research question, the criteria are explained in Table 2. Following these predetermined stage of inclusion and exclusion criteria, only papers explicitly addressing the cybersecurity capabilities approach were considered. Given the meaning embedded in the term "capability" in this paper and taking into consideration that technological, organizational, and managerial capability scholars have used this term in a variety of different ways (e.g., web service policy capability, information processing capabilities, data analytics capacity, and detection capability, among others), empirical papers were sought that contained a theoretical and practical basis on capabilities that promote the processes that are directed toward a change in a firm's resource base (Eisenhardt & Martin, 2000; Helfat et al., 2009; Teece et al., 1997).

Furthermore, meta-synthesis is limited to case studies that make a substantive contribution to cybersecurity capabilities with the potential to change, perform or innovate in cybersecurity. This follows premise developed by seminal authors (Eisenhardt & Martin, 2000; Teece et al., 1997) that firm internal position concerns the firm's stock of, technological, reputational, procedural, financial, and structural assets, whilst external position concerns the institutional market and environment in which the firm operates. The last step entailed reducing the sample to studies whose a priori research question or purpose refers to the cybersecurity field and capabilities that have an impact on changing and performing cybersecurity outcomes. Applying this strict criterion means that evidence was not collected incidentally.

All the studies showed a clear link between theory and empirical evidence and reflected the methodological standards that scholars such as Yin (2014), Eisenhardt (1989), Eisenhardt and Graebner, 2007 and Hoon (2013) have instilled in the field. Overall, forty-seven case studies met the inclusion criteria in the meta-synthesis. Appendix B presents a list of all case studies (included/excluded) in the meta-synthesis and the variables in focus, capabilities involved, and empirical context. Following Hoon (2013), the studies that were synthesized aimed to at extend or build theory with the use of multiple data sources following a clear research question. Entailing in this meta-synthesis using different case studies designs, ranging from inductive theory building to the extended method, it seeks to identify methods of analysis and consistent research strategies, with the best recommended practices (Eisenhardt, 1989; Eisenhardt & Graebner, 2007; Hoon, 2013; Yin, 2014).

Table 2. Inclusion and Exclusion Criteria

Criteria	Rationales	Reasons for Exclusion
Only Case Study	The criterion ensures that there is no difference in the methodological approach that the primary researchers claim to have used.	Papers with in-depth illustrative examples on how a framework works or not to understand capabilities in cybersecurity. In addition, any papers that primary relying on quantitative data.
Framing cybersecurity capabilities approach	Organizational, managerial, and technological capabilities in cybersecurity reflect a firm's ability to change and perform through process design and security controls to reach higher levels of cyber protection.	Relying on conceptual organizations, other capabilities not associated with cybersecurity, heuristics, purely experimental or not associated with a cybersecurity perspective.
Referring to the processes of cybersecurity	Identify cybersecurity capabilities as a strong capacity to overcome information security challenges. This entails the inclusion of papers that provide a substantive contribution of cybersecurity capabilities in firm's change and performance.	Without focus on cybersecurity capabilities or its applications and development.
Focusing on priori goals, research question, and research interests	The research question(s) or goal(s) in cybersecurity should provide focus on the technological, organizational, or managerial capabilities to explain changes in the cybersecurity scenario.	Other cybersecurity perspective not including capabilities as the initial main research objective.
Check quality	According to standards and guidelines (Eisenhardt, 1989; Yin, 2014), the studies were analyzed in terms of rigorous reporting style, clear linkage between theory and empirical evidence, clear contextualization, multiple data sources, and clarity concerning the theoretical purpose.	No further exclusions due to quality assessment.
Note: Adapted from Hoon (2013).		

4.4 Extracting and Coding Data

In this step (step 4), the focus is to extract, code, and categorize evidence from the studies under synthesis (Hoon, 2013; Noblit & Hare, 1997). The meta-synthesis is based on what original researchers have constructed according to their interpretation of the primary data and context. These insights constitute the 'data' of this meta-synthesis. Using the recommended guidelines found in the literature of qualitative research, this paper seeks qualitative rigor and systematically transfers raw data into theoretical interpretations (Corley & Gioia, 2004; Gioia et al., 2013).

Each primary case study was coded for the descriptive characteristics such as type of paper design, setting, population sample, or data sources. After completing the code extractions, the individual coding was merged into a combined database into Atlas.ti software offering a broad range of coding characteristics, which was beneficial as it not only informed about the specific nature of the body of studies under synthesis but also sensitized for potentially relevant contextual factors (Hoon, 2013).

The attribution of names to each code followed the recommendation to assign a code with a name semantically as close as possible to the concept it describes (Miles & Huberman, 1994). A coding structure (Barbosa et al., 2013) is developed to compromise three parts:

[N]- [cc]- [mmm]- [Name of the capability], being

→ [N] sequential number within the capability category

→ [cc] the mnemonic of a two-letter code which represents the second order outcomes in cybersecurity capabilities related to DO = doing, IM= improving, EN= enabling, MA= managing as DCCI second-order dimensions.

→ [mmm] the mnemonic of a three-letter code which refers to first order outcomes in cybersecurity capabilities related to ESR = Engineering Cybersecurity Requirements, DCS = Designing Cybersecurity Solutions, RDE = Reviewing Cybersecurity Design, SDA = Standardizing

Cybersecurity Activities, ISD = Improving Cybersecurity; SSA = Supporting Cybersecurity Activities; PMS = Planning and Managing Cybersecurity and MWO = Managing Stakeholders as DCCI first-order outcomes.

→ [name of the capability] defines the capability with a name to enable to identify it quickly and easily, embedding in the case study data set.

Concepts and practical evidence of cybersecurity capabilities were coded in Atlas.ti software and aligned with the meaning of the construct overlapped significantly with the DC approach for IS research (Steininger et al., 2022) and Capability Maturity Model Integration (Al-Matouq et al., 2020; CMMI Institute, 2019). The listed events, factors, and patterns occurred around the "cybersecurity capabilities" as well as how they influenced, facilitated, or hindered the "adjustment of change and performance of firms." Appendix C provides the synthesized structure of the total of 734 codes identified to generate the DCCI model and an example of codification in a case study. To ensure consistency while coding, any discrepancies that emerged were carefully documented in the coding database and resolved by discussions with two additional specialists with experience in information security and academic methods and further rereading of the original studies (Xiao et al., 2019). The emergent codes were subsequently fed into the coding structure. Overall, working with a coding process helps to reduce errors in data recording and avoid the omission of relevant material (Hoon, 2013; Miles & Huberman, 1994).

4.5 Analyzing on a paper-specific level

The process of data analysis in step 5 is iterative in order to improve insights and generalizability (Eisenhardt & Graebner, 2007). Constant comparative techniques and the combination of open, axial, and selective coding were used to analyze the case studies data. As initial coding to develop first-order outcomes, the "induction" of the logical data analysis process is applied by adhering to the case studies' wording and terms (Gioia et al., 2013). The codes captured variables such as 'information security governance,' 'big data analytics capabilities,' 'computing capacity,' and 'knowledge protection'. The list of variables captured among the case studies are shown in Appendix B. These codes were assigned to words, sentences or even paragraphs in the margins of the text of papers. The process of coding data continued until no further distinct, shared patterns among the data were found, i.e., theoretical saturation was reached (Eisenhardt & Graebner, 2007). For example, the axial code 'Managing Stakeholders' were captured by open codes emerged from examples about high attention is given to training human resources (Corallo et al., 2012); convincing users to accept the integrated nature of the system (Seethamraju, 2015), open communication channels to all relevant stakeholders (Ahmad et al., 2021), among others.

The next phase, the "abduction;" that is, the existing literature and scientific knowledge are consulted to analyze and develop definitions that explain the data. Data reanalysis is used by acting as knowledgeable agents and using centric concepts. Focusing on the deep structure underlying the first-order outcomes and the similarities and differences between them, a reduction of the first-order outcomes to more abstract second-order dimensions (firm's change and performance) was achieved by using the structure of DCs developed by Steinning et al. (2022). In total, eight first-order cybersecurity capabilities were identified, using as guidance the structure developed by Al-Mantouq et al. (2020). During the final phase, the data was further analyzed by investigating the possibility of aggregating the cybersecurity capabilities identified in second-order dimensions to form more abstract outcomes at a higher level (aggregate dimensions) (Corley & Gioia, 2004; Gioia et al., 2013; H. Naseer et al., 2021).

By doing so, the first-order outcomes were combined into four aggregate dimensions that captured the overarching capabilities relevant for understanding the role of DCCI. In accordance with Naseer et al. (2020), the data structure supports revalidating the final description back to the underlying data and established a clear connection between data, the emerging capabilities, and the aggregate dimensions. By keeping the voices of both informants and researchers, we could rigorously develop detailed and accurate definitions of concepts from the data (H. Naseer et al., 2021).

4.6 Synthesis of DCCI at a Cross-Paper Level

From a paper-specific level to a cross analysis, this step (step 6) merges the capabilities identified in each case study into a meta-network. This network provides the foundation to explore consonant and dissonant aspects of cybersecurity capabilities across the studies through a comparative exercise (Hoon, 2013; Miles & Huberman, 1994). A meta network goes beyond the individual studies to allow mechanisms,

causalities, or conditions and their outcomes emerge from the analysis across a set of studies. Appendix C provides the synthesized structure of codes in DCCI capabilities after concluding the iterations of first-order outcomes and second-order dimensions for each case study. Therefore, a meta network emerged gathering a pattern of a sequencing o meaningful capabilities found across the case studies.

5 Results of Meta-synthesis

As a result (step 7), this meta-synthesis reveals the description of four second-order dimensions and eight first-order outcomes of DCCI and their implications from managerial perspectives (Table 3). In the table, beyond the references described in Section 3, we show the main perspective that DCs clustered as capacities: (1) sensing to identify and assess opportunities and threats; (2) seizing to mobilize resources addressing opportunities or threats and capturing value from doing so; and (3) transforming to continue renewal (Teece, 2007, 2012) to categorize the capabilities found across the case studies. Sensing, seizing, and transforming involve higher-level practices that enable a firm to change its resources in order to achieve organizational performance to survive and grow (Steininger et al., 2022). The organizational change prompted by DCs is what leads to organizational performance. The DCCI framework, therefore, seeks to explain what processes and abilities are extended and renewed to create a strategic cybersecurity intelligence that coevolves with the business environment. Therefore, capabilities, resources, and cybersecurity intelligence jointly determine the firm's competitiveness in cybersecurity phenomena (Steininger et al., 2022; Teece, 2018). Each dimension is analyzed and discussed in sequence, presenting evidence found in the literature.

In 'doing cybersecurity', a second-order dimension, software development life cycle is crucial, and cybersecurity is one of the most relevant software quality characteristics (Al-Matouq et al., 2020), and inevitable for all kinds of software projects (Humayun et al., 2022), although it varies from project to project because firms tend to consider it as an afterthought (Al-Matouq et al., 2020). According to Humayun et al. (2022), "when bugs and defects are discovered early in the production process, they are easier and less expensive to fix than those discovered later". Therefore, cybersecurity must be incorporated into the system development life cycle, i.e., from the beginning until the software is deployed in its business environment (Al-Matouq et al., 2020; Humayun et al., 2022) because many devices might be interconnected if software needs to work as an integral part of an overall system, for instance. This dimension is also vital for ensuring the security, safety, and reliability of communications among countless interconnected technologies (Ghobakhloo & Fathi, 2019), considering the nature of building, controlling and reviewing cybersecurity design, solutions and activities.

The 'improving cybersecurity' perspective encompasses network, data, application security and individual cyber-hygiene practices (Kapoor et al., 2021; Tanwar et al., 2018). Therefore, to avoid complexity and cybersecurity failure, it is necessary to consider process of experimentality (attempt or experiment with a course of action to acquire a security outcome), manage security across multiple systems and ability for a higher level of collaborative software development (Abdul Molok et al., 2018; Goode & Lacey, 2021; H. Naseer et al., 2021). In this dimension, it is crucial to handle resource change and reconfiguration to mitigate cyber threat surroundings (Al-Matouq et al., 2020; Eisenhardt & Martin, 2000; Helfat et al., 2009; Steininger et al., 2022; Teece, 2007).

As security events are not always predicted (Eastman et al., 2015; A. Naseer et al., 2021; H. Naseer et al., 2021), the 'enabling cybersecurity' dimension supports the complexity of cyber events as a trigger of monitoring function, where security teams can proactively respond to them as they occur by taking effective usage of DCCI against possible threats and potential consequences (A. Naseer et al., 2021). In this dynamic or highly unpredictable threat landscape, security teams experience high degrees of uncertainty and have a greater need for both real-time information and capacity to process it. Thus, in cyber threat environments, supporting cybersecurity activities becomes valuable as it enables firms to look at all types of events and rule out false positives, determining which are real incidents or breaches to respond in a proactive way (A. Naseer et al., 2021; Steininger et al., 2022).

The 'managing cybersecurity' dimension recognizes the far-reaching transformational role that cybersecurity solutions may provide to firms. Creating cybersecurity solutions that can quickly integrate automate investigations, intelligence data and forensic analysis applying complex algorithms and visual analytics to discover the potential threats helps to improve agility in security processes and execute innovative security strategies that can better deal with the dynamic cyber threat environment. The far-reaching potential of cyber risks also increases demand for more data integration, visualization,

automation, analytics, and stakeholders' awareness. Therefore, firms who develop cybersecurity solutions need to carefully consider these requirements when developing their DCCI (A. Naseer et al., 2021).

Table 1. DCCI Framework

2nd order	1st order	DC	DCCI Description	Managerial Implications	Outcome
Doing Cybersecurity	Engineering Cybersecurity Requirements	Sensing	P = Depict process of systems architecture (physical, electronic relationships); establish infrastructure (mechanisms and processes) to detect threats; build technological support to anticipate security risks; allow automation security through other trust solutions and associated technologies; establish and document a path in cyber defense; identification of technological developmental trends, peer influences in security architecture, variations and security technical foresightedness based on market orientation; allocation of physical and virtual resources to build security architecture.	Existing cybersecurity solutions need to be replaced or integrated in complex ways, which leads to investments. Therefore, new infrastructures and adaptations of technological legacy must be part of the work agenda to meet critical challenges posed by risks with cyber-attacks.	OC
	Designing Cybersecurity Solutions	Sensing	P = Development of security steps and processes; identification of security gaps; preparedness of data quality; understanding security control process; foster adequate security solutions and control identification for business requirements; advocacy of security changes and their effective implementation, contributing to no long security implementation time; use market and users' requirements to design new security solutions; define mechanisms of problem resolution in case of incompatibilities, application restrictions, malfunctions, and industry standards.	Identify and rank business processes based on information security criticality in line with their relevance to the business reduce the impact of risks because by performing some prioritization, it is possible to decide which processes are most critical starting with relatively low risk ones, as pilot projects, and increase protection against cyberattacks.	OC
	Reviewing Cybersecurity Design	Sensing	P = Validate security mechanisms; seek analytical information; review security policy procedures; check technology readiness to ensure a secure environment; apply current security knowledge to obtain benefits rather than conceptualize, collect, or only codify; introduce proper activities to revise security designs; analysis for cybersecurity threats and incidents from multiple sources to detect patterns between different threats and incidents	Managers engaged with technological readiness to many challenges of information security such as heterogeneous devices, standards, protocols; various layers of data sources and volumes must translate their security mechanisms across multiple threat intelligence sources such as monitoring policies or data analytics reports.	OC

Improving Cybersecurity	Standardizing Cybersecurity Activities	Seizing	P = Discern new security risks in the environment to standardized interface and protocols; deployment of standard security policies; configure security across multiple systems, monitor, permit or restrict virtual accessibility; define security measures; facilitate the implementation and standardization of other security controls or services; support security progressively embedded within normal business operational processes and an integrated system for cyber-risks management; use of proven tools and data analytics to prevent incidents, breaches and penalties.	The reduction of cybersecurity risks is directly associated with resources visibility in relation to their location and ownership. Thus, the standardization of activities in information security improves the level of trust in accesses authorization.	OC
	Improving Cybersecurity	Sensing	P = Enhance experimentality (attempt or experiment with a course of action to acquire security outcome); exchanging security information, knowledge about communication channels to maintain closer relationships between trading partners to facilitate information flow; ensure threat hunting (reinforce process of proactive and iterative detection, isolation, and mitigation of advanced threats that are not detected by traditional security controls); continuous security improvements following recommendations from official entities.	The experimentation of technologies, in pilot projects, allowed the identification of pros and cons about their adoption, and also allowed rapid progress in a later official implementation. Because it's a lot of work to remediate cybersecurity projects or overcome barriers of rejection from users. It's best to start any effort with a historical foundation formed by past experience to foster collaborative security posture.	OC OP
		Transforming	A = Promote experiment or research analysis to new security controls for the purpose of institutionalization and transformation of the security posture; foster collaboration with other software development firms and security exercises in the practice of joint decision-making as different security authority levels come into play; insert awareness of change in security requirements, the perception of changes in the environment and opportunity capture of the market and institutional environment.		

Enabling Cybersecurity	Supporting Cybersecurity Activities	Transforming	P = Continuous monitoring and data analytics to understand cyber risks; perform event and log collection and correlation; forensic data acquisition; responsibility sharing to release secure software, secure infrastructure, institutional processes and mechanisms to guide appropriate specified secure information in all aspects of business; establish command and control to facilitate timely data sharing (communication) and information management (intelligence, which involves collecting, analyzing, and disseminating the relevant information). A = Discern all types of events and rule out false positives; determine which ones are real incidents or breaches and be able to address these through an incident response process; alternativity knowledge (conceive of alternate interpretations circumstances or realities); discuss security incidents and responsibilities for risk mitigation, develop or implement security policy with support and engagement of a security steering committee; develop a common perception of possible threats and potential consequences to responding to security incidents in the future	Understanding the nature and advantages of cybersecurity actions in order to generously support the development of technologies and initiatives associated with data security is always an indispensable driving force for strengthening a strong information security posture. And it can determine the outcome of decisions across the organization and provide resource direction for new adoption processes.	OC
Managing Cybersecurity	Planning & Managing Cybersecurity	Seizing	P = Define a form of governing security service level (confidentiality and partners' agreements, hierarchical structure of roles and responsibilities); use a flat and flexible organizational structure to maintain security activities; provide identity and action knowledge (create or alter a security identity for the purpose of an action), for example, become involved politically, establish government involvement, legislation balance, disclosure of security risk to the organization, develop security governance processes; tracking key risk indicators through dynamic risk assessment; develop and implement an action plan to meet security maturity criteria. A = Usability of historical insights on a real-time basis (on demand and continuous) to separately determine how best to plan and manage cybersecurity in the future; be aware of the whole cyber threat landscape; leverage cyber threat intelligence to understand the capability, opportunity, and intent of malicious actors.	Switching to a security model often requires careful planning to ensure productivity and that data access needed for daily work is maintained. Therefore, a planning in cybersecurity will shape the feature requirements and drive the selection of the evaluation metrics for a potential technology provider, compliance requisites, legal implications adjusting the business expectations based on the risks appetite.	OC

	Managing Stakeholders	Seizing	A = Balance cyber risk against ability to compel stakeholders to configure their security settings correctly and consistently; understand motivations and security knowledge behind stakeholders' actions and develop security strategies that are aligned with the organizational culture; cultivate a trusting, collaborative and knowledge sharing security culture to create capabilities to address security difficulties; use decision making driven by data analytics to develop a firmer tone of management intent, clearer guidelines regarding what constitutes risk tolerance or risk appetite and be able to deliver meaningful insights that can empower the decision makers to take the appropriate timely action; play a pivotal role in spreading formal cybersecurity stakeholders' education to create new security capabilities.	The various stakeholders have their own goals and motivations in addition to the shared goals and conflicts of interest arise and each party is vulnerable. Therefore, to avoid unfavorable behavior, managers need to know how to work under uncertainties and enhance the level of trust in cybersecurity to surpass the perceived risk from stakeholders. This will ensure that confidence in cybersecurity intelligence will flourish. Within a competitive society, the various company stakeholders cannot enter into partnerships with blind trust, believing that everyone will do the right thing.	OC / OP

Notes: Combinative descriptions based on case study findings, discussion sections.
Legend: OC= Organizational Change; OP = Organizational Performance; P = Processes; A = Abilities.
Adapted from Abdul Molok et al., 2018; Ahmad et al., 2021; Akinsanya et al., 2019; Al-Matouq et al., 2020; Attili et al., 2018; Bartnes and Moe, 2017; Bradford et al., 2014; Cahyani et al., 2017; Diaz et al., 2019; Goles et al., 2008; Goode and Lacey, 2021; Laamanen and Wallin, 2009; Magnuson et al., 2004; Mathrani and Lai, 2021; Naseer, Maynard, et al., 2021; Renwick and Gleasure, 2021; Seethamraju, 2015; Tan et al., 2016; Wang et al., 2019; Williams et al., 2013.

For this multi-dimensionality of capabilities, it is valuable to think about institutional complexity, which may subject firms to multiple, competing, and contradictory cybersecurity logics (Bartnes & Moe, 2017; Williams et al., 2013). Therefore, it would be acceptable for connecting processes and abilities in cybersecurity requirements to involve a critical capabilities framework in both 'horizontal connections' (cooperative and competitive) and 'vertical connections' (power and authority) to highlight the need to "shift the analytic focus from individual firms to higher levels of analysis" as identified by [(Scott, 2008), p. 441-442] and [(Goles et al., 2008), p. 316].

Given the sensitive nature of cybersecurity issues, only a dynamic multi-dimensional process (Williams et al., 2013) cannot be the way to fully resolve cyber threats, as the involvement of humans (mainly cybersecurity managers) is critical to investigating and confirming these threats, particularly when they are internal (H. Naseer et al., 2021). Therefore, understanding the processes and ability in the proposed DCCI framework (See Table 3) may increase the potential for a new meaning surfacing in terms of the prospective and retrospective aspects of cybersecurity governance, compliance and risk management, thereby enriching firms' strategies in this field (Williams et al., 2013).

Overall, creating cyber threat intelligence (Ahmad et al., 2021; H. Naseer et al., 2021; Schlette et al., 2021) requires data analytics to understand the intention, capability, and opportunity used by malicious actors. The strong willingness of firms to develop DCCI should consider that the 'capability' of a malicious actor is the means used in the malicious activity, 'opportunity' is the vulnerabilities that it can exploit, and 'intention' reflects the desire to target assets (H. Naseer et al., 2021). Although, after understanding these aspects an "unorthodox" way of thinking is required (Steinmetz, 2015) and the presence of DCCI to support this new way of thinking is extremely important when it comes to building cyber threat intelligence. In other words, to deal with both unpredictable threats (e.g. insider data theft, advanced persistent threats,

and zero-day attacks) and predictable threats (e.g., trojan attacks, distributed denial of service, and phishing attacks), firms most of the time encounter an uncertain cyber landscape in terms of process, systems and capabilities, in which only a strong DCCI framework can support the needs for a successful resource configuration (H. Naseer et al., 2021).

Ahmad et al. (2021), mentioned that cyber threat intelligence helps to direct situation awareness of the threat environment. H. Naseer et. al (2021) highlighted predictive insights used by firms to understand what was likely to happen in the cyber threat environment in the future. The authors emphasize “a combination of threat hunting, anomaly detection, continuous monitoring, findings from descriptive, forensic, real-time insights, and dynamic risk assessment mechanisms were used to generate these predictive insights”. They enhance cybersecurity awareness, forecast future trends, and craft the “ideal course of action” to proactively deal with unpredictable cybersecurity threats. However, the accuracy of these predictive insights is highly dependent on data quality and the modelling technique, which is why predictive models require careful treatment, continuous optimization and DCCI presence (Ahmad et al., 2021; H. Naseer et al., 2021). Figure 1 presents the holistic view of the proposed DCCI framework.

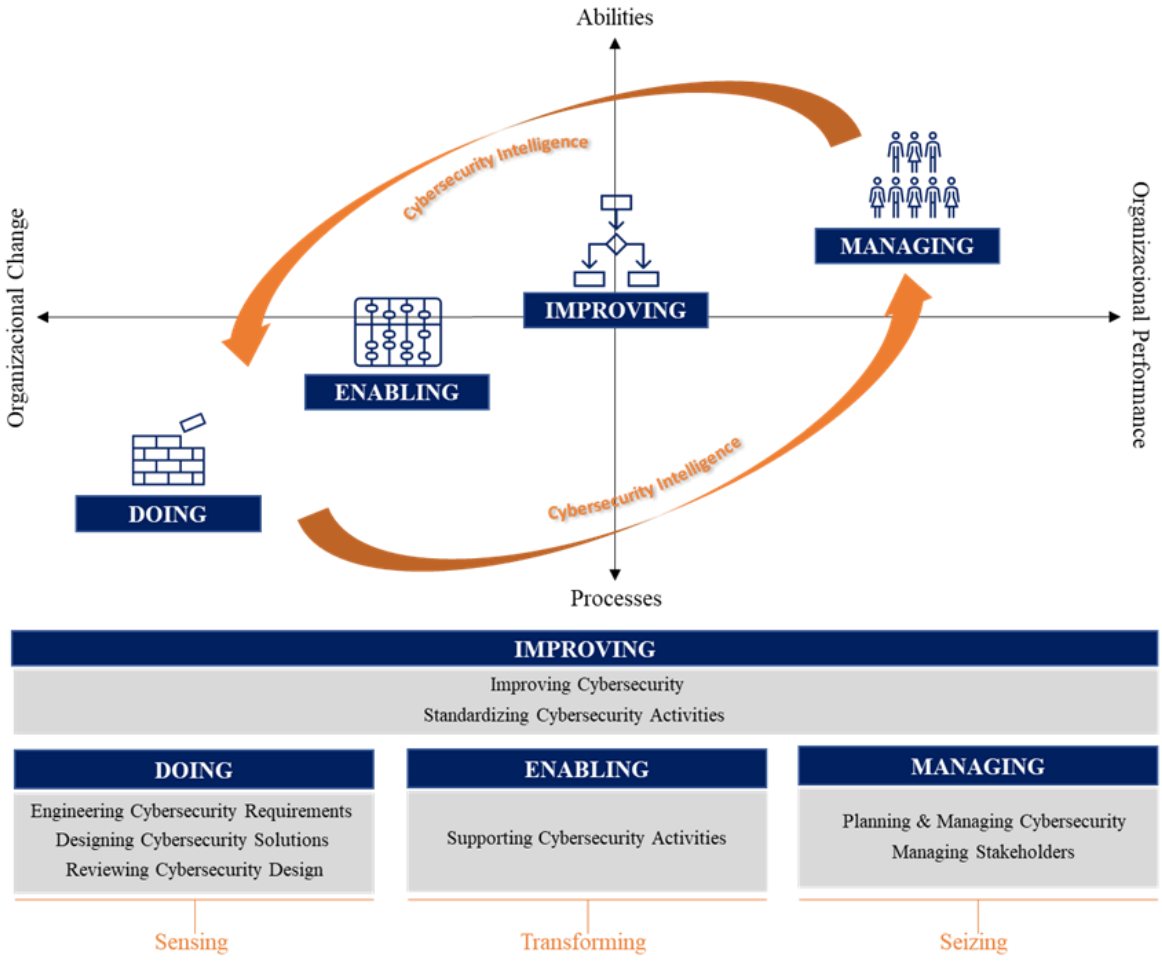

Figure 1. DCCI Framework

6 Discussion about results

The last step of the meta-synthesis (step 8) has to do with general limitations about heterogeneity in the primary studies or the way the meta-synthesis led to the findings is an aspect to which specialists pay attention (Hoon, 2013). Being very inclusive regarding the studies that are incorporated entails the risks of increasing the range of interpretations of a phenomenon and not allowing an appropriate analysis. Therefore, the discussion with specialists was based on recommendations of level of agreement above 0.70 (Boudreau et al., 2001) in the codification process of dynamics capabilities where two other

researchers coded 10 papers and a comparison of codes demonstrated 0.79 of agreement in interrater in the process. Additionally, two rounds of discussion about the framework were realized to confirm its adherence in business practices. The specialists have more than 10 years' experience in cybersecurity and have been working in international companies as practitioners and in universities as academics. Thus, we believe that our outcome constitutes a valuable contribution to the development of DCCI because it goes beyond recent reviews of DCs (Paradza & Daramola, 2021; Steininger et al., 2022), offering an empirical consolidation based on an exhaustive search strategy with a high quality method and criteria.

Considering that this paper offers a structure of synthesis that emerges from the interpretation and translation of practical positions and outcomes stemming from cybersecurity research, specialists were questioned about their applicability and contribution of the key variables, constructs, and underlying relationships. In this vein, the feedback was totally positive, and specialists mentioned that it was the first time that they were seeing a too realistic representation of capabilities in cybersecurity. We also explained that across a set of primary qualitative case studies to reach an extended and refined new viewpoint for DCCI, the meta-synthesis performed in this research had a major potential to synthesize evidence on a particular topic in real cases to build theory, rather than reviewing the existent intellectual literature to formulate new research questions or future research directions (Hoon, 2013; Tranfield et al., 2003). Thus, synthetizing evidence in different business context has potential to affirm that DCCI enhance firms' change and performance against cyber risks to support a more deductive theory test based on the foundations and descriptions provided in the framework and moving to higher levels of abstraction (Eisenhardt & Graebner, 2007; Hoon, 2013; Shah & Corley, 2006).

Finally, specialists also mentioned about the beneficial role of this DCCI framework in defining future actions to develop capabilities across IT teams because it is something firms do not know how and where to start investing their time and efforts to adopt a cybersecurity posture. Therefore, this meta-synthesis may be also most beneficial to adequate future quantitative measures (Edmondson & Mcmanus, 2007) regarding DCCI, considering that within a field that is progressing like this a meta-synthesis is helpful in converging this growing body of knowledge into new insight. For example, more intermediate fields such as the dynamic capabilities approach are particularly promising for meta-synthesis, where a continuously increasing body of empirical studies explores theoretical relationships and/or new constructs. However, it is not only the number of studies analyzed that justifies the choice of a meta-synthesis; instead, it is the fresh insights that a synthesis may bring to a field that legitimates its course of action (Cooper, 2017; Hoon, 2013).

7 Conclusion

The rise of DCCI is inevitable in the process of cybersecurity phenomena based on the human capabilities chain. This meta-synthesis revealed case studies of successful and failed information security activities and, based on the practical examples pointed out, we designed a framework, which is also useful for different business sectors. The DCCI framework presented four second-order dimensions and eight first-order capabilities based on forty-seven case studies, which might serve as a valuable reference and provide late-comers with an opportunity for the development of cross-dimensional cybersecurity intelligence through building DCCI.

The empirical references provided in Table 3 showed that the dynamic capabilities in cybersecurity generated a level of cybersecurity intelligence in the businesses in question (at least an innovation, change or performance). Moving from theory to practice, this meta-synthesis enhanced the visibility of DCCI, answering our research question concerning whether cybersecurity can be introduced and incorporated as a complementary view in a perspective of dynamic capabilities. In Appendix B, we show how technological, organizational, and managerial capabilities shaped DCCI across the studies.

Discussions surrounding the second-order dimensions and meta-synthesis robustness show that understanding and adhering to the applicability of each DCCI can help firms to learn more effectively about cybersecurity practices, processes, and abilities. The journey to develop and achieve DCCI will certainly include unforeseen challenges, and critical adjustment will aid the implementation of this framework.

Theoretical Contribution. Our paper adds to the current knowledge by presenting a conceptual understanding underpinned by relevant theories and empirical evidence. First, we identified the salient features of DCs in IS research and explained how these features play a critical role in enabling firms to

change and perform in terms of cybersecurity. We organized and synthesized the main cybersecurity capabilities that help organizations to balance their efforts across the reactive and initiative-taking approaches of developing cybersecurity intelligence processes. Second, following the recommendations of Hoon (2013) for performing a meta-synthesis, we examined how these cybersecurity capabilities change firms that reconfigure resources and processes to detect and respond to unknown, unpredictable, and new cybersecurity threats. Specifically, the DCCI framework provides descriptions of abilities and processes that firms may see and thus improve their overall cybersecurity changes and performance. Our paper addressed the research question by developing the DCCI framework (see Table 3) that provides a complementary view of DCs and demonstrates cybersecurity change and performance by using a contingent resource-based view (technological, organizational, and managerial capabilities).

Practical Contribution. The findings indicate possible managerial implications, particularly in information security planning and management. As security concerns seem to be more about technological aspects (resources and processes) than the effective use of DCCI, firms might develop practical strategies to ease the development of DCCI, such as security standardization, by adopting policies consistently for security settings and promoting a steering committee to align engineering security requirements with existing ones. DCCI are also considered a way of enhancing security features for all business stakeholders. The framework also provides overall guidance for the sustainable development of DCCI and may contribute to making investments in these sorts of capabilities, not only by firms but also by governments and research institutions.

Limitations. There may be a limitation due to restricting the method to forty-seven case studies published in the selected journals rather than the set of 438 publications initially identified in this research field. Case studies, given the difficulty to produce large and multiple different methods, also have to do with "the generality of the results with respect to a specific population" (Diaz et al., 2019; van Heesch et al., 2012; Seaman, 1999). However, forty-seven case studies were sufficient to validate claims of important contributions regarding cybersecurity principles and DCCI to explain new avenues for DCs. Even with limitations, this is important for the life cycle of security software development, in which external factors may affect the outcomes of adoptions.

Future research. To confirm the proposed DCCI framework, further studies with large samples could validate the links between constructs with regard to how firms change and perform with regard to cybersecurity challenges. Future studies could include the development of model measurements in different research contexts, and the addition of the newly suggested factor of information security and control for testing. Moreover, other theories (e.g., “Technology-Organization-Environment”) and online tools to explain DCCI from different perspectives or in various contexts (e.g., large enterprises, supply chain, different regions, and industries) could be included.

To sum up, as this meta-synthesis demonstrates the versatility of DCCI in firms' change and performance, they may want to consider using DCCI to strengthen trust in addition to branding and business reputation. This could involve developing DCs related to unorthodox strategies and other investments to enhance cybersecurity practices.

Acknowledgments

This research was funded by Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brazil (CAPES), grant number 001”.

References

Abdul Molok, N. N., Ahmad, A., & Chang, S. (2018). A case analysis of securing organisations against information leakage through online social networking. *International Journal of Information Management*, *43*, 351–356. https://doi.org/10.1016/j.ijinfomgt.2018.08.013

Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review*, *5*(1). https://www.timreview.ca/article/861

Aguinis, H., Dalton, D. R., Bosco, F. A., Pierce, C. A., & Dalton, C. M. (2011). Meta-Analytic Choices and Judgment Calls: Implications for Theory Building and Testing, Obtained Effect Sizes, and Scholarly Impact. *Journal of Management*, *37*(1), 5–38. https://doi.org/10.1177/0149206310377113

Aguinis, H., Hill, N. S., & Bailey, J. R. (2021). Best Practices in Data Collection and Preparation: Recommendations for Reviewers, Editors, and Authors. *Organizational Research Methods*, *24*(4), 678–693. https://doi.org/10.1177/1094428119836485

Aguinis, H., Ramani, R. S., & Alabduljader, N. (2020). Best-Practice Recommendations for Producers, Evaluators, and Users of Methodological Literature Reviews. *Organizational Research Methods*, 109442812094328. https://doi.org/10.1177/1094428120943281

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How can organizations develop situation awareness for incident response: A case study of management practice. *Computers & Security*, *101*, 102122. https://doi.org/10.1016/j.cose.2020.102122

Akbari, M., Khodayari, M., Khaleghi, A., Danesh, M., & Padash, H. (2021). Technological innovation research in the last six decades: A bibliometric analysis. *European Journal of Innovation Management*, *24*(5), 1806–1831. https://doi.org/10.1108/EJIM-05-2020-0166

Akinsanya, O. O., Papadaki, M., & Sun, L. (2019). Towards a maturity model for health-care cloud security. *Information & Computer Security*, *28*(3), 321–345. https://doi.org/10.1108/ICS-05-2019-0060

Al-Matouq, H., Mahmood, S., Alshayeb, M., & Niazi, M. (2020). A Maturity Model for Secure Software Design: A Multivocal Study. *IEEE Access*, *8*, 215758–215776. https://doi.org/10.1109/ACCESS.2020.3040220

Amit, R., & Schoemaker, P. J. H. (1993). Strategic assets and organizational rent: Strategic Assets. *Strategic Management Journal*, *14*(1), 33–46. https://doi.org/10.1002/smj.4250140105

Attili, V. S. P., Mathew, S. K., & Sugumaran, V. (2018). Understanding Information Privacy Assimilation in IT Organizations using Multi-site Case Studies. *Communications of the Association for Information Systems*, *42*. https://doi.org/10.17705/1CAIS.04204

Aytug, Z. G., Rothstein, H. R., Zhou, W., & Kern, M. C. (2012). Revealed or concealed? Transparency of Procedures, Decisions, and Judgment Calls in Meta-Analyses. *Organizational Research Methods*, *15*(1), 103–133. https://doi.org/10.1177/1094428111403495

Barbosa, A. F., Pozzebon, M., & Diniz, E. H. (2013). Rethinking e-government performance assessment from a citizen perspective: E-gov performance from a citizen perspective. *Public Administration*, n/a-n/a. https://doi.org/10.1111/j.1467-9299.2012.02095.x

Barney, J. B., Nelson, R. R., & Winter, S. G. (1987). An Evolutionary Theory of Economic Change. *Administrative Science Quarterly*, *32*(2), 315. https://doi.org/10.2307/2393143

Barreto, I. (2010). Dynamic Capabilities: A Review of Past Research and an Agenda for the Future. *Journal of Management*, *36*(1), 256–280. https://doi.org/10.1177/0149206309350776

Bartnes, M., & Moe, N. B. (2017). Challenges in IT security preparedness exercises: A case study. *Computers & Security*, *67*, 280–290. https://doi.org/10.1016/j.cose.2016.11.017

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management: A Procedure Model and its Application. *Business & Information Systems Engineering*, *1*(3), 213–222. https://doi.org/10.1007/s12599-009-0044-5

Becker, J., Niehaves, B., Poeppelbuss, J., & Simons, A. (2010). *Maturity models in IS research*. 42. pdf. https://aisel.aisnet.org/ecis2010/42

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, *63*(4), 531–540. https://doi.org/10.1016/j.bushor.2020.03.010

Boudreau, M.-C., Gefen, D., & Straub, D. W. (2001). Validation in Information Systems Research: A State-of-the-Art Assessment. *MIS Quarterly*, *25*(1), 1. https://doi.org/10.2307/3250956

Bradford, M., Earp, J. B., & Grabski, S. (2014). Centralized end-to-end identity and access management and ERP systems: A multi-case analysis using the Technology Organization Environment framework. *International Journal of Accounting Information Systems*, *15*(2), 149–165. https://doi.org/10.1016/j.accinf.2014.01.003

BSIMM. (2022). *BSMM12: Building security in maturity model. [Online].* https://www.bsimm.com/download.html

Burisch, R., & Wohlgemuth, V. (2016). Blind spots of dynamic capabilities: A systems theoretic perspective. *Journal of Innovation & Knowledge*, *1*(2), 109–116. https://doi.org/10.1016/j.jik.2016.01.015

Cahyani, N. D. W., Martini, B., Choo, K.-K. R., & Al-Azhar, A. M. N. (2017). Forensic data acquisition from cloud-of-things devices: Windows Smartphones as a case study: Forensic Data Acquisition from Cloud-of-Things Devices. *Concurrency and Computation: Practice and Experience*, *29*(14), e3855. https://doi.org/10.1002/cpe.3855

Carlson, K. D., & Ji, F. X. (2011). Citing and Building on Meta-Analytic Findings: A Review and Recommendations. *Organizational Research Methods*, *14*(4), 696–717. https://doi.org/10.1177/1094428110384272

Catota, F. E., Granger Morgan, M., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity*, *5*(1), 1–19. https://doi.org/10.1093/cybsec/tyz001

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, *9*(1), 70–104. https://doi.org/10.1080/10864415.2004.11044320

Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, *15*(5/6), 358–368. https://doi.org/10.1108/09576050210447046

CMMI Institute. (2019). *Introducing CMMI Security v2.0. [Online].* https://cmmiinstitute.com/cmmi/sec

Cooper, H. M. (2017). *Research synthesis and meta-analysis: A step-by-step approach* (Fifth edition). Sage.

Corallo, A., Lazoi, M., & Secundo, G. (2012). Inter-organizational knowledge integration in Collaborative NPD projects: Evidence from the aerospace industry. *Knowledge Management Research & Practice*, *10*(4), 354–367. https://doi.org/10.1057/kmrp.2012.25

Corley, K. G., & Gioia, D. A. (2004). Identity Ambiguity and Change in the Wake of a Corporate Spin-off. *Administrative Science Quarterly*, *49*(2), 173–208. https://doi.org/10.2307/4131471

Cortina, J. M. (2003). Apples and Oranges (and Pears, Oh My!): The Search for Moderators in Meta-Analysis. *Organizational Research Methods*, *6*(4), 415–439. https://doi.org/10.1177/1094428103257358

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Dalton, D. R., & Dalton, C. M. (2008). Meta-Analyses: Some Very Good Steps Toward a Bit Longer Journey. *Organizational Research Methods*, *11*(1), 127–147. https://doi.org/10.1177/1094428107304409

D'Arcy, J., Adjerid, I., Angst, C. M., & Glavas, A. (2020). Too good to be true: Firm social performance and the risk of data breach. *Information Systems Research*, *31*(4), 1200–1223. https://doi.org/10.1287/isre.2020.0939

Dhillon, G., Smith, K., & Dissanayaka, I. (2021). Information systems security research agenda: Exploring the gap between research and practice. *The Journal of Strategic Information Systems*, *30*(4), 101693. https://doi.org/10.1016/j.jsis.2021.101693

Diaz, J., Perez, J. E., Lopez-Pena, M. A., Mena, G. A., & Yague, A. (2019). Self-Service Cybersecurity Monitoring as Enabler for DevSecOps. *IEEE Access*, *7*, 100283–100295. https://doi.org/10.1109/ACCESS.2019.2930000

Doyle, K. (2018). *Introducing CMMI Development v2.0 to Pan-India Spin*. CMMI Institute; pdf. https://www.coursehero.com/file/57060596/CMMI-V2-0-Technical-Overviewpdf/

Dube, D. P., & Mohanty, R. P. (2020). Towards development of a cyber security capability maturity model. *International Journal of Business Information Systems*, *34*(1), 104. https://doi.org/10.1504/IJBIS.2020.106800

Eastman, R., Versace, M., & Webber, A. (2015). Big data and predictive analytics: On the cybersecurity front line. *IDC Whitepaper, February*. http://v2.itweb.co.za/whitepaper/Whitepaper_SAS_Cyber_Security.pdf

Edmondson, A. C., & Mcmanus, S. E. (2007). Methodological fit in management field research. *Academy of Management Review*, *32*(4), 1246–1264. https://doi.org/10.5465/amr.2007.26586086

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review*, *14*(4), 532–550.

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory Building from Cases: Opportunities And Challenges. *Academy of Management Journal*, *50*(1), 25–32. https://doi.org/10.5465/amj.2007.24160888

Eisenhardt, K. M., & Martin, J. A. (2000). Dynamic capabilities: What are they? *Strategic Management Journal*, *21*(10–11), 1105–1121. https://doi.org/10.1002/1097-0266(200010/11)21:10/11<1105::AID-SMJ133>3.0.CO;2-E

Gërguri-Rashiti, S., Ramadani, V., Abazi-Alili, H., Dana, L.-P., & Ratten, V. (2017). ICT, Innovation and Firm Performance: The Transition Economies Context: ICT, Innovation and Firm Performance. *Thunderbird International Business Review*, *59*(1), 93–102. https://doi.org/10.1002/tie.21772

Ghaffari, F., & Arabsorkhi, A. (2018). A New Adaptive Cyber-Security Capability Maturity Model. *2018 9th International Symposium on Telecommunications (IST)*, 298–304. https://doi.org/10.1109/ISTEL.2018.8661018

Ghobakhloo, M., & Fathi, M. (2019). Corporate survival in Industry 4.0 era: The enabling role of lean-digitized manufacturing. *Journal of Manufacturing Technology Management*, *31*(1), 1–30. https://doi.org/10.1108/JMTM-11-2018-0417

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods*, *16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Goles, T., White, G. B., & Dietrich, G. (2008). Dark screen: An exercise in cyber security. *MIS Quarterly Executive*, *4*(2), 5. https://aisel.aisnet.org/misqe/vol4/iss2/5

Goode, S., & Cruise, S. (2006). What Motivates Software Crackers? *Journal of Business Ethics*, *65*(2), 173–201. https://doi.org/10.1007/s10551-005-4709-9

Goode, S., & Lacey, D. (2021). Exploiting organisational vulnerabilities as dark knowledge: Conceptual development from organisational fraud cases. *Journal of Knowledge Management*. https://doi.org/10.1108/JKM-01-2021-0053

Helfat, C. E., Finkelstein, S., Mitchell, W., Peteraf, M., Singh, H., Teece, D., & Winter, S. G. (2009). *Dynamic Capabilities: Understanding Strategic Change in Organizations*. John Wiley & Sons. https://books.google.com.br/books?id=u0Tuh5vixLkC

Helfat, C. E., & Winter, S. G. (2011). Untangling Dynamic and Operational Capabilities: Strategy for the (N)ever-Changing World. *Strategic Management Journal*, *32*(11), 1243–1250. https://doi.org/10.1002/smj.955

Hock-Doepgen, M., Clauss, T., Kraus, S., & Cheng, C.-F. (2021). Knowledge management capabilities and organizational risk-taking for business model innovation in SMEs. *Journal of Business Research*, *130*, 683–697. https://doi.org/10.1016/j.jbusres.2019.12.001

Hoon, C. (2013). Meta-Synthesis of Qualitative Case Studies: An Approach to Theory Building. *Organizational Research Methods*, *16*(4), 522–556. https://doi.org/10.1177/1094428113484969

Humayun, M., Jhanjhi, N., Fahhad Almufareh, M., & Ibrahim Khalil, M. (2022). Security Threat and Vulnerability Assessment and Measurement in Secure Software Development. *Computers, Materials & Continua*, *71*(3), 5039–5059. https://doi.org/10.32604/cmc.2022.019289

IBM Security. (2021). *Cost of a Data Breach Report 2021* (p. 73). https://www.ibm.com/security/data-breach

Iyengar, K., Sweeney, J. R., & Montealegre, R. (2015). Information Technology Use as a Learning Mechanism. *Mis Quarterly*, *39*(3), 615–642. https://www.jstor.org/stable/26629623

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. *Journal of Medical Internet Research*, *20*(5). https://doi.org/10.2196/10059

Jalali, M. S., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *Journal of Strategic Information Systems*, *28*(1), 66–82. https://doi.org/10.1016/j.jsis.2018.09.003

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598

Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions. *Sustainability*, *14*(1), 8. https://doi.org/10.3390/su14010008

Kisamore, J. L., & Brannick, M. T. (2008). An Illustration of the Consequences of Meta-Analysis Model Choice. *Organizational Research Methods*, *11*(1), 35–53. https://doi.org/10.1177/1094428106287393

Kolini, F., & Janczewski, L. J. (2022). Exploring Incentives and Challenges for Cybersecurity Intelligence Sharing (CIS) across Organizations: A Systematic Review. *Communications of the Association for Information Systems*, *50*(1), 86–121. https://doi.org/10.17705/1CAIS.05004

Kour, R., & Karim, R. (2020). Cybersecurity workforce in railway: Its maturity and awareness. *Journal of Quality in Maintenance Engineering*, *27*(3), 453–464. https://doi.org/10.1108/JQME-07-2020-0059

Kwon, J., & Johnson, M. E. (2014). Proactive Versus Reactive Security Investments in the Healthcare Sector. *MIS Quarterly*, *38*(2), 451-A3. https://www.jstor.org/stable/26634934

Laaksonen, O., & Peltoniemi, M. (2018). The Essence of Dynamic Capabilities and their Measurement: Essence of Dynamic Capabilities. *International Journal of Management Reviews*, *20*(2), 184–205. https://doi.org/10.1111/ijmr.12122

Laamanen, T., & Wallin, J. (2009). Cognitive Dynamics of Capability Development Paths. *Journal of Management Studies*, *46*(6), 950–981. https://doi.org/10.1111/j.1467-6486.2009.00823.x

Lee, O.-K., Sambamurthy, V., Lim, K. H., & Wei, K. K. (2015). How Does IT Ambidexterity Impact Organizational Agility? *Information Systems Research*, *26*(2), 398–417. https://doi.org/10.1287/isre.2015.0577

Leukfeldt, R., Kleemans, E., & Stol, W. (2017). The Use of Online Crime Markets by Cybercriminal Networks: A View from Within. *American Behavioral Scientist*, *61*(11), 1387–1402. https://doi.org/10.1177/0002764217734267

Magnuson, J. A., Klockner, R., Ladd-Wilson, S., Zechnich, A., Bangs, C., & Kohn, M. A. (2004). Security Aspects of Electronic Data Interchange Between a State Health Department and a Hospital Emergency Department: *Journal of Public Health Management and Practice*, *10*(1), 70–76. https://doi.org/10.1097/00124784-200401000-00012

Mathrani, S., & Lai, X. (2021). Big Data Analytic Framework for Organizational Leverage. *Applied Sciences*, *11*(5), 2340. https://doi.org/10.3390/app11052340

McCormack, K., Willems, J., van den Bergh, J., Deschoolmeester, D., Willaert, P., Indihar Štemberger, M., Škrinjar, R., Trkman, P., Bronzo Ladeira, M., Paulo Valadares de Oliveira, M., Bosilj Vuksic, V., & Vlahovic, N. (2009). A global investigation of key turning points in business process maturity. *Business Process Management Journal*, *15*(5), 792–815. https://doi.org/10.1108/14637150910987946

Merigó, J. M., Gil-Lafuente, A. M., & Yager, R. R. (2015). An overview of fuzzy research with bibliometric indicators. *Applied Soft Computing*, *27*, 420–433. https://doi.org/10.1016/j.asoc.2014.10.035

Mikalef, P., Pateli, A., & van de Wetering, R. (2021). IT architecture flexibility and IT governance decentralisation as drivers of IT-enabled dynamic capabilities and competitive performance: The moderating effect of the external environment. *European Journal of Information Systems*, *30*(5), 512–540. https://doi.org/10.1080/0960085X.2020.1808541

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook* (2. ed., [Nachdr.]). Sage.

Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Masood Siddiqui, A. (2021). Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis. *International Journal of Information Management*, *59*, 102334. https://doi.org/10.1016/j.ijinfomgt.2021.102334

Naseer, H., Maynard, S. B., & Desouza, K. C. (2021). Demystifying analytical information processing capability: The case of cybersecurity incident response. *Decision Support Systems*, *143*, 113476. https://doi.org/10.1016/j.dss.2020.113476

Ngwum, N. I. (2016). *Information Security Maturity Model (ISMM)* [University of Manchester]. pdf. https://www. researchgate.net/publication/292607439_Information_Security_Maturity_Model_ISMM

Noblit, G. W., & Hare, R. D. (1997). *Meta-Ethnography: Synthesizing qualitative studies* (3. ed). Sage.

Paradza, D., & Daramola, O. (2021). Business Intelligence and Business Value in Organisations: A Systematic Literature Review. *Sustainability*, *13*(20), 11382. https://doi.org/10.3390/su132011382

Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information & Management*, *52*(2), 183–199. https://doi.org/10.1016/j.im.2014.08.008

Pavlou, P. A., & El Sawy, O. A. (2006). From IT Leveraging Competence to Competitive Advantage in Turbulent Environments: The Case of New Product Development. *Information Systems Research*, *17*(3), 198–227. https://doi.org/10.1287/isre.1060.0094

Piccoli & Ives. (2005). Review: IT-Dependent Strategic Initiatives and Sustained Competitive Advantage: A Review and Synthesis of the Literature. *MIS Quarterly*, *29*(4), 747. https://doi.org/10.2307/25148708

Pratt, M. G. (2008). Fitting Oval Pegs into Round Holes: Tensions in Evaluating and Publishing Qualitative Research in Top-Tier North American Journals. *Organizational Research Methods*, *11*(3), 481–509. https://doi.org/10.1177/1094428107303349

Rea-Guaman, A. M., San Feliu, T., Calvo-Manzano, J. A., & Sanchez-Garcia, I. D. (2017). Comparative Study of Cybersecurity Capability Maturity Models. Em A. Mas, A. Mesquida, R. V. O'Connor, T. Rout, & A. Dorling (Orgs.), *Software Process Improvement and Capability Determination* (Vol. 770, p. 100–113). Springer International Publishing. https://doi.org/10.1007/978-3-319-67383-7_8

Renwick, R., & Gleasure, R. (2021). Those who control the code control the rules: How different perspectives of privacy are being written into the code of blockchain systems. *Journal of Information Technology*, *36*(1), 16–38. https://doi.org/10.1177/0268396220944406

Rodgers, W., Attah-Boakye, R., & Adams, K. (2020). Application of Algorithmic Cognitive Decision Trust Modeling for Cyber Security Within Organisations. *IEEE Transactions on Engineering Management*, 1–10. https://doi.org/10.1109/TEM.2020.3019218

Rosoff, H., Cui, J., & John, R. S. (2013). Heuristics and biases in cyber security dilemmas. *Environment Systems and Decisions*, *33*(4), 517–529. https://doi.org/10.1007/s10669-013-9473-2

Rousseau, D. M., Manning, J., & Denyer, D. (2008). Evidence in management and organizational science: Assembling the field's full weight of scientific knowledge through syntheses (SSRN scholarly paper 1309606). *Social Science Research Network, Rochester*.

Schlette, D., Vielberth, M., & Pernul, G. (2021). CTI-SOC2M2 – The quest for mature, intelligence-driven security operations and incident response capabilities. *Computers & Security*, *111*, 102482. https://doi.org/10.1016/j.cose.2021.102482

Scott, W. R. (2008). Approaching adulthood: The maturing of institutional theory. *Theory and Society*, *37*(5), 427–442. https://doi.org/10.1007/s11186-008-9067-z

Seaman, C. B. (1999). Qualitative methods in empirical studies of software engineering. *IEEE Transactions on Software Engineering*, *25*(4), 557–572. https://doi.org/10.1109/32.799955

Sedgewick, A. (2014). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0* (NIST CSWP 02122014; p. NIST CSWP 02122014). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.02122014

Seethamraju, R. (2015). Adoption of Software as a Service (SaaS) Enterprise Resource Planning (ERP) Systems in Small and Medium Sized Enterprises (SMEs). *Information Systems Frontiers*, *17*(3), 475–492. https://doi.org/10.1007/s10796-014-9506-5

Shah, S. K., & Corley, K. G. (2006). Building Better Theory by Bridging the Quantitative?Qualitative Divide. *Journal of Management Studies*, *43*(8), 1821–1835. https://doi.org/10.1111/j.1467-6486.2006.00662.x

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Spicer, J. (2019). Cybercriminal Profiling. *EDPACS*, *60*(3), 1–17. https://doi.org/10.1080/07366981.2019.1675965

Steininger, D. M., Mikalef, P., Pateli, A., & Ortiz-de-Guinea, A. (2022). Dynamic Capabilities in Information Systems Research: A Critical Review, Synthesis of Current Knowledge, and Recommendations for Future Research. *Journal of the Association for Information Systems*, *22*(2), 447–490. https://doi.org/10.17705/1jais.00736

Steinmetz, K. F. (2015). Craft(y)ness: An Ethnographic Study of Hacking. *British Journal of Criminology*, *55*(1), 125–145. https://doi.org/10.1093/bjc/azu061

Tan, K. H., Wong, W. P., & Chung, L. (2016). Information and Knowledge Leakage in Supply Chain. *Information Systems Frontiers*, *18*(3), 621–638. https://doi.org/10.1007/s10796-015-9553-6

Tanwar, S., Vora, J., Tyagi, S., Kumar, N., & Obaidat, M. S. (2018). A systematic review on security issues in vehicular ad hoc network. *Security and Privacy*, *1*(5), e39. https://doi.org/10.1002/spy2.39

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*, *28*(13), 1319–1350. https://doi.org/10.1002/smj.640

Teece, D. J. (2012). Dynamic Capabilities: Routines versus Entrepreneurial Action: Routines versus Entrepreneurial Action. *Journal of Management Studies*, *49*(8), 1395–1401. https://doi.org/10.1111/j.1467-6486.2012.01080.x

Teece, D. J. (2018). Dynamic capabilities as (workable) management systems theory. *Journal of Management & Organization*, *24*(3), 359–368. https://doi.org/10.1017/jmo.2017.75

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, *18*(7), 509–533. https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z

Tran, H. K. V., Börstler, J., bin Ali, N., & Unterkalmsteiner, M. (2022). How good are my search strings? Reflections on using an existing review as a quasi-gold standard. *E-Informatica Software Engineering Journal*, *16*(1), 220103. https://doi.org/10.37190/e-Inf220103

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. https://doi.org/10.1111/1467-8551.00375

Valdez-Juárez, L. E., & Castillo-Vergara, M. (2020). Technological Capabilities, Open Innovation, and Eco-Innovation: Dynamic Capabilities to Increase Corporate Performance of SMEs. *Journal of Open Innovation: Technology, Market, and Complexity*, *7*(1), 8. https://doi.org/10.3390/joitmc7010008

van Heesch, U., Avgeriou, P., & Hilliard, R. (2012). A documentation framework for architecture decisions. *Journal of Systems and Software*, *85*(4), 795–820. https://doi.org/10.1016/j.jss.2011.10.017

Wade & Hulland. (2004). Review: The Resource-Based View and Information Systems Research: Review, Extension, and Suggestions for Future Research. *MIS Quarterly*, *28*(1), 107. https://doi.org/10.2307/25148626

Wang, W., Cao, Q., Qin, L., Zhang, Y., Feng, T., & Feng, L. (2019). Uncertain environment, dynamic innovation capabilities and innovation strategies: A case study on Qihoo 360. *Computers in Human Behavior*, *95*, 284–294. https://doi.org/10.1016/j.chb.2018.06.029

Williams, S. P., Hardy, C. A., & Holgate, J. A. (2013). Information security governance practices in critical infrastructure organizations: A socio-technical and institutional logic perspective. *Electronic Markets*, *23*(4), 341–354. https://doi.org/10.1007/s12525-013-0137-3

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *CPA Journal*, *74*(12), 38–42. https://digitalcommons.kennesaw.edu/facpubs

Xiao, J., Wu, Y., Xie, K., & Hu, Q. (2019). Managing the e-commerce disruption with IT-based innovations: Insights from strategic renewal perspectives. *Information & Management*, *56*(1), 122–139. https://doi.org/10.1016/j.im.2018.07.006

Yin, R. K. (2014). *Case study research: Design and methods* (5. edition). SAGE.

Zahra, S. A., Sapienza, H. J., & Davidsson, P. (2006). Entrepreneurship and Dynamic Capabilities: A Review, Model and Research Agenda*. *Journal of Management Studies*, *43*(4), 917–955. https://doi.org/10.1111/j.1467-6486.2006.00616.x

Zollo, M., & Winter, S. G. (2002). Deliberate Learning and the Evolution of Dynamic Capabilities. *Organization Science*, *13*(3), 339–351. https://doi.org/10.1287/orsc.13.3.339.2780

Appendix A: Source Title Ranking

Table A1. Main Source Publications

Journal Title	Publications
Journal of the Association for Information Systems	13
Communications of the Association for Information Systems	10
Computers & Security	10
IEEE Access	4
International Journal of Information Management	4
International Journal of Medical Informatics	4
MIS Quarterly Executive	4
Pacific Asia Journal of The Association for Information Systems	4
Sustainability	4
Decision Support Systems	3
Information Systems Frontiers	3
International Journal of Production Research	3
Journal of Knowledge Management	3
Business Process Management Journal	2
Computer Communications	2
Contemporary Security Policy	2
Information and Software Technology	2
International Journal of Computer Integrated Manufacturing	2
International Journal of Human Resource Management	2
International Journal of Technology Management	2
Journal of Information Technology	2
Journal of Management Studies	2
Journal of Manufacturing Technology Management	2
Journal of Systems and Software	2
Knowledge Management Research & Practice	2
Security and Communication Networks	2
Others	55

Appendix B: Papers Retrieved from Inclusion and Exclusion Criteria

Table B1. Papers Analyzed

Authors	Main variables under attention	Capability	Inclusion Exclusion Criteria	Empirical Context
Er et al., 2022	Trust-aware process design (input, people, process, and output)	OM	0	GoFood Company, a food delivery company in Indonesia
Humayun et al., 2022	Security Best Practices in system development life cycle	T	0	Organization XYZ
Kapoor et al., 2021	Ransomware Defense (detection, avoidance, and mitigation)	T	0	The infamous Djvu ransomware case
Hsu et al., 2021	Telemedicine	OM	1	At NewYork Presbyterian, a nonprofit healthcare network
Wu & Plakhtii, 2021	Cloud computing technology in higher education	TOM	1	Sechenov First Moscow State Medical University (Russia), Prydniprovska State Academy of Civil Engineering and Architecture (Ukraine) and Wuxi Institute of Technology (China)
Rukanova et al., 2021	Value of Data Analytics in Government Supervision	OM	2	PROFILE research project funded
Stacey et al., 2021	Emotional responses for cybersecurity	T	2	Global manufacturing company
Al-Matari et al., 2021	Information Security Management Model	OM	0	Retirement organization and public telecommunication corporation in the Republic of Yemen.
Zhang et al., 2021	Multi-chain blockchain architecture to enhance the transaction processing capability	T	0	Hotel Booking Winding Tree and Hyperledger Fabric in the tourism industry
Gong & Janssen, 2021	Big Data Analytics	TOM	0	Dutch Tax and Customs Administration in the Netherlands
Goode & Lacey, 2021	Dark Knowledge (ability to identify organizational weaknesses, vulnerabilities, and compromise points)	TOM	0	A large Asia-Pacific telecommunications provider
Mathrani & Lai, 2021	Big Data Analytics process and capabilities	TOM	0	Two companies are China-based (large smartphone manufacturer and electricity generation and retailing compliance), and one is from New Zealand (fast-moving consumer goods business segment).
Naseer, Naseer, et al., 2021	Real-time analytics Capability (complex event processing, decision automation, and on-demand and continuous data analysis)	TOM	0	Twenty cybersecurity experts interviews
Renwick & Gleasure, 2021	Privacy Attitudes (Privacy-related concepts, resources, and methods for blockchain technologies)	TOM	0	Monero, a cryptocurrency community
Smith et al., 2021	Agile techniques into the Cyber Security domain of	TOM	0	Protecting Industrial Control Systems

	incident response			
Ahmed et al., 2021	Situation Awareness in incident response	OM	0	Large multinational finance organization
Naseer, Maynard, et al., 2021	Information processing capability in cybersecurity incident response	TOM	0	Twenty-seven participants, drawn from three financial sector firms
Hosseini et al., 2020	Vulnerability and Recoverability capabilities	T	1	The first case study is a single supplier with three states operational, semi-operational and fully disrupted. Second case study is comprised of a single manufacturer and two suppliers supply leather and RFID blocking chip.
Tigharsi et al., 2019	Labor Mobility	OM	2	12 employees in different industries
Brous & Janssen, 2020	Mature data governance capability	OM	0	A large European public organization projects in Road management and Electrical Grid Management
Akinsanya et al., 2019	Health-care cloud security	TOM	0	Hospitals' cyber security internal processes
Ghobakhloo & Fathi, 2019	Hybrid lean-digitized manufacturing system	TOM	0	Small manufacturing firm
Al-Matouq et al., 2020	Secure Software Design Maturity Model	TOM	0	Two software organizations in Saudi Arabia
Montealegre et al., 2019	Digital Infrastructure Ambidexterity	TOM	2	RE/MAX LLC, a global real estate franchise
Diaz et al., 2019	Security practices (Build, run and monitor) in a DevOps environment.	T	0	At the Universidad Polytechnic de Madrid as part of a demonstrator for a smart campus.
Johansson et al., 2019	Assuring Information Security (Correctness, Confidentiality, Accessibility)	T	0	Digital railway maintenance development company and its main customer
Li et al., 2019	Healthcare Big Data Governance Practices	TOM	0	Ten typical regional health information networks in China
Wang et al., 2019	Dynamic innovation capabilities and innovation strategies	TOM	0	Internet security industry
Holen-Rabbersvik et al., 2018	Communication and Information Sharing	M	1	Inter-municipal healthcare services
Abdul Molok et al., 2018	Leakage Mitigation Capability	OM	0	Four Firms in Malaysia at various levels of maturity in relation to the security management of Online Social Networking
Chatfield & Reddick, 2019	Crowdsources software bug detection	OM	0	Pentagon vulnerability reward program or bug bounty program
D'Orazio & Choo, 2018	Security Mechanisms in mobile platforms and apps	T	0	Eighteen popular iOS cloud apps
Lu & Sinnott, 2018	Access control policy	T	0	Australasian Pediatric Endocrine Group and the Juvenile Diabetes Research Foundation
Attili et al., 2018	Privacy Capabilities (Information Privacy and Privacy Assimilation)	TOM	0	Eighteen IT organizations in India and USA
Hall et al., 2017	Implementation of monitoring	M	1	Three dementia-specialist

	technologies in care homes			care homes in North-West England
Dang-Pham et al., 2017	Behavioral information security	OM	1	A large organization in Vietnam
Rehm et al., 2017	Networking Capabilities	OM	2	Cooperative research project called SmartNets partly funded by the European Commission
Aoki & Wilhelm, 2017	Ambidexterity	OM	2	Toyota Motor Corporation
Oguntala et al., 2017	Poor adoption of cloud computing	OM	2	African Entreprise in Nigeria
Ritchie et al., 2017	Telehealth-based ergonomics service delivery process	T	2	Alberta-based non-profit advocacy group
Wu et al., 2017	Geographic video surveillance	T	2	144 Hospitals listed in Taiwan Joint Commission on Hospital Accreditation
Mani et al., 2017	Big Data Analytics	TOM	2	Surat Milk Union Limited firm, Gujarat, India
Bartnes & Moe, 2017	Security Incidents Preparedness	OM	0	Norwegian Distribution System Operators
Cahyani et al., 2017	Mobile Forensic Tool Capabilities	T	0	Windows phone (cloud-of-things device)
Rashidi & Rezakhani, 2017	Attribute based access control	T	0	Enterprises IT managers
Tan et al., 2016	Knowledge and Information Leakage	OM	0	Five manufacturing companies in Malaysia
Wang et al., 2016	Social Media Apps (SMA) Capabilities, B2B communication and business performance.	TOM	0	Five case study conducted with senior managers/owners of SME (Small and Medium Enterprises) in B2B context
Cr&all & Allan, 2015	Estonia's Norm-building in cybersecurity	OM	1	Estonian government norms
Krishnan & Vorobyov, 2015	Access Control	T	1	E-voting Protocols
Jin et al., 2015	International R&D alliances	OM	2	Chinese local firms in telecommunication industry
Lei & Moon, 2015	Decision Support System for market-driven product positioning and design	T	2	US automotive market data
Seethamraju, 2015	ERP Systems (backup mechanisms and service continuity measures)	TOM	0	Four firms in India : steel products manufacturing company; power infrastructure and project management company; energy company; automobile manufacturing company; and a SaaS ERP vendor
Blanco et al., 2015	Secure Data Warehouse repository	T	0	A Sales department
Jiang & Okamoto, 2014	China's national search engine.	OM	2	Jaike Company
Patel et al., 2014	Food security Status	OM	2	Street food sector in Madura, India.
Bradford et al., 2014	End-to-end identity and Access management	TOM	0	Two large higher educational institutions

Hughes & Chapel, 2013	Internal social collaboration platform called the Hub	OM	1	KPMG
Piekkari et al., 2013	Translation behavior	OM	2	Nordic Bank
Yu et al., 2013	Web Service Policy Security Capabilities	TOM	0	Four security requirements cases on Web service
Williams et al., 2013	Information Security Governance	OM	0	Fourteen Australian critical infrastructure organizations
Corallo et al., 2012	Knowledge Protection (Human Resources Awareness, Legal Structure, Alliance Process)	OM	0	Two Italian aerospace firms
Aissani et al., 2012	Learning Capabilities	T	0	Multi-site companies supply chain planning
Desouza, 2011	Security Intellectual Mgmt (Source, Analytics, Interpretation, Action)	OM	1	Executives involved in security management programs in twenty-three firms
Barletta et al., 2011	Access Control in Web Services	T	0	e-business Banking Service and Digital Contract Signing in the e-government area
Batra et al., 2010	Agile methods and the traditional structured	OM	2	Cruise Line Industry
Knoerich, 2010	Cross-border acquisitions by companies	OM	2	Chinese acquisitions of German firms in the machinery and equipment industry
Kumar et al., 2010	Sourcing Decisions	OM	2	US manufacturer of industrial thermal transfer bench-top printer
Zhen et al., 2010	Collaborative virtual assembly scheme based on grid technology	T	2	A car-assembly workstation
de Leusse et al., 2010	Collaborative Engineering (policy enforcement, identity brokerage, access management and security governance)	TOM	0	Service Oriented Enterprise in Aerospace industry
Chen et al., 2009	Secure Access Control	OM	0	An automobile component producer
Laamanen & Wallin, 2009	Capabilities Development	TOM	0	Three network security software firms
Krogh et al., 2008	IT-intensive mortgage bank	OM	2	IndyMac Bank
Mathiassen & Pedersen, 2008	Management of uncertainty in organic systems development	OM	2	SoftConsult, a large Scandinavian supplier of IT-based solutions
Ranganathan & Balaji, 2007	IS Offshore Outsourcing Capabilities (Systemic Thinking, Vendor Management, Resource Management, and Change Management)	OM	2	Eighteen firms in IS offshore outsourcing
El Sawy & Pavlou, 2008	IT-enabled Business Capabilities (operational, dynamic, and improvisational)	TOM	2	Six Chief Information Systems Officer interviews
Gorrieri et al., 2008	Multicast communication and security issues	T	0	Gennaro and Rohatgi protocols
Bauer et al., 2007	Mobile TV	OM	2	Mobile TV in South Korea
Freed et al., 2007	In-House Systems Design	OM	2	Semicondutor Firm
Vrontis et al., 2006	Strategic review of the marketing function	OM	2	Cypriot company operating in the liquid food packaging industry

Goles et al., 2008	Dark Screen (level of awareness, coordinating interorganizational responses, cyber incidents communications channels)	OM	0	Dark Screen exercise
Petrovic-Lazarevic & Sohal, 2004	CIO's ethical behavior	OM	2	Two Australian companies
Magnuson et al., 2004	Security Project	TOM	0	Hospital emergency department and a state public health department in Oregon
Chien et al., 2003	Computing Capacity (Physical Node Management, Resource Scheduling, and Job Management)	T	0	Entropia distributed computing system case
Smith et al., 2021	Wireless technology	OM	2	A Santa Clara University study of ten firms currently using mobile computing in a variety of ways
Verwoerd & Hunt, 2002	Security Verification Technique	T	0	Government Organization
Leizerov, 2000	Privacy Groups' Internet Protest Tactics	OM	2	Intel's controversial launch of the Pentium III® processor
Dyerson & Mueller, 1999	Technological Capabilities Building	OM	2	Department of Social Security in UK
Bailey et al., 1998	Asset-light strategy	OM	2	Hotels in Markowitz's mixed assets portfolios
Sayers, 1995	Basic skills programs	TOM	2	Texas Instruments Defense Systems Corporation and SGS-Thomson Microelectronics; Abbott Laboratories, J & E Die Casting, and Company X

Notes: Legend of Capabilities: T = Technological; O = Organizational; M = Managerial
Legend of Inclusion / Exclusion Criteria: 0 = Included
1 = It does not develop arguments about cybersecurity capabilities
2 =Theme is out of scope (not related to cybersecurity)

Appendix C: Dynamic Capabilities in Cybersecurity Identified in the Case Studies

Figure C1 shows a coding structure approach in Atlas.ti in a case study. It is only codified relevant evidence extracted according to the impact of organizational, managerial, and technological capabilities to promote change and performance in cybersecurity approach of the firms to create cybersecurity intelligence. Each cybersecurity capability is identified and computed being organized under the theoretical approach of the Capability Maturity Model Integration (2019) that enables firms to build, assess, and improve their processes and capabilities in cybersecurity and the Building Security in Maturity Model (2022) that quantified the security practices of many firms. This framework is represented in Table C1.

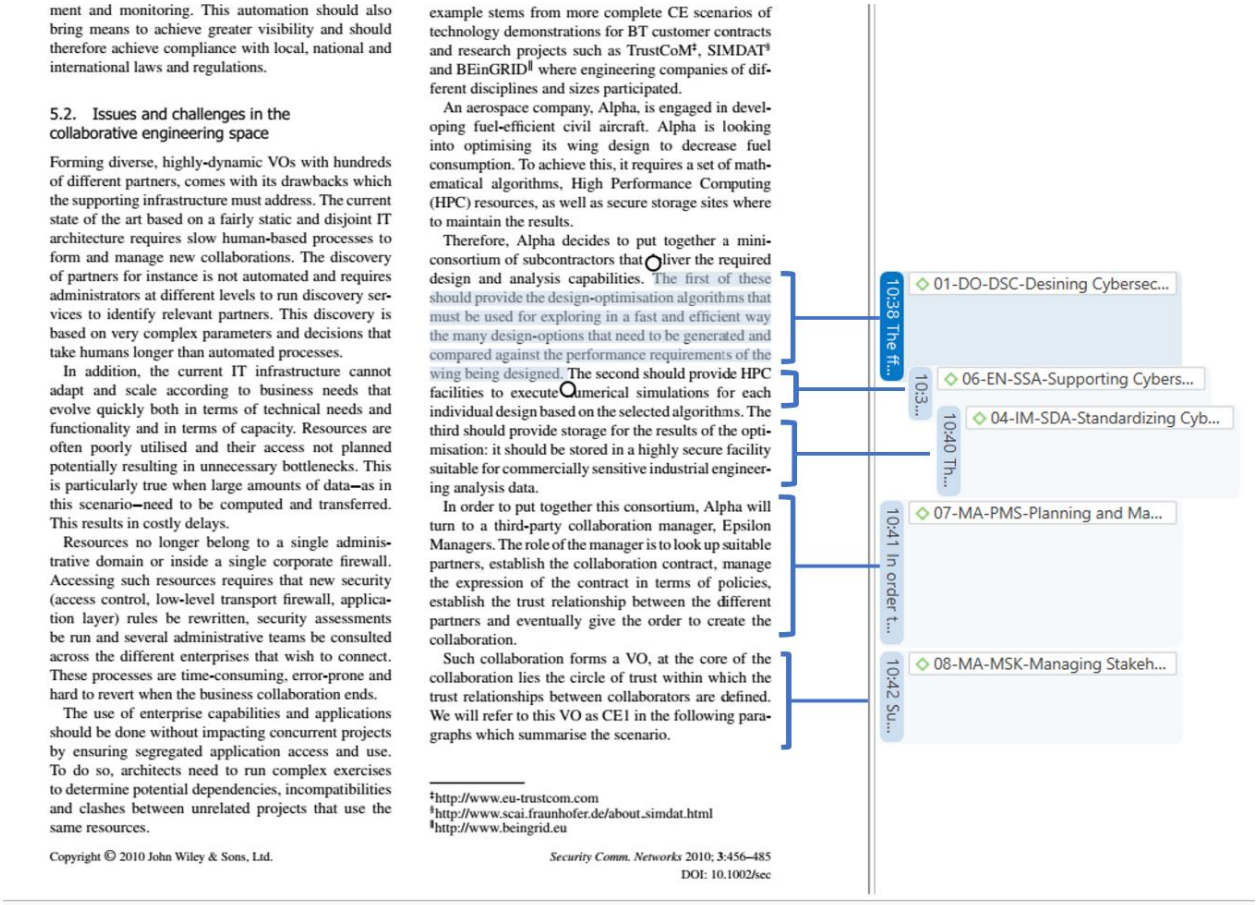

Figure C2. Coding Structure Approach in a case study using Atlas.ti Software

Table C1. Codes Framework by Paper Included

Authors	DO-ESR	DO-DCS	DO-RDE	IM-DSA	EN-ISD	EN-SSA	MA-PMS	MA-MSK
Abdul Molok et al. ,2018	0	3	0	0	0	3	2	3
Ahmad et al., 2021	0	1	1	12	5	2	14	5
Aissani et al., 2012	4	5	0	0	1	0	0	0
Akinsanya et al., 2019	2	1	0	1	0	0	1	0
Al-Matari et al., 2021	11	9	0	3	0	3	4	3
Al-Matouq et al., 2020	0	2	0	1	0	0	0	1
Barletta et al., 2011	0	5	0	0	0	0	0	0
Bartnes & Moe, 2017	2	0	0	1	5	2	0	1
Blanco et al., 2015	0	10	0	1	0	1	0	0
Bradford et al., 2014	2	2	2	5	3	2	4	0
Brous & Janssen, 2020	1	0	0	1	2	0	6	0
Cahyani et al., 2017	0	0	13	0	0	1	2	0
Chatfield & Reddick, 2019	0	1	0	2	4	1	2	1
Chen et al., 2009	0	2	0	3	0	0	3	0
Chien et al., 2003	0	0	0	0	0	0	0	0
Corallo et al., 2012	1	1	0	1	0	1	1	2
de Leusse et al., 2010	7	9	1	7	1	6	9	1
Diaz et al., 2019	8	6	0	1	0	8	1	0
D'Orazio & Choo, 2018	20	0	0	1	2	0	0	0
Ghobakhloo & Fathi, 2019	0	0	0	1	0	0	3	0
Goles et al., 2008	4	0	0	2	1	2	6	4
Gong & Janssen, 2021	6	3	0	4	3	6	4	0
Goode & Lacey, 2021	0	0	0	0	0	0	0	8
Gorrieri et al., 2008	0	14	0	0	0	0	0	0
Humayun et al., 2022	15	6	1	3	2	1	0	1
Johansson et al., 2019	0	2	0	1	0	0	0	0
Kapoor et al., 2021	0	0	0	1	0	2	0	1
Laamanen & Wallin, 2009	1	1	0	2	2	0	5	2
Li et al., 2019	3	3	1	4	1	1	3	3
Lu & Sinnott, 2018	0	2	0	2	0	0	0	0
Magnuson et al., 2004	3	4	0	4	8	0	4	2
Er et al., 2022	1	4	0	4	1	0	2	3
Mathrani & Lai, 2021	9	8	0	11	0	3	1	0
H. Naseer et al., 2021	1	0	5	2	8	9	10	5
A. Naseer et al., 2021	2	1	0	0	0	4	1	0
Attili et al., 2018	5	2	0	2	6	0	4	16
Rashidi & Rezakhani, 2017	2	3	0	0	0	0	0	0
Renwick & Gleasure, 2021	2	5	0	1	2	2	1	3
Seethamraju, 2015	0	3	1	1	1	1	2	4
Smith et al., 2021	1	2	0	1	3	1	1	0
Tan et al., 2016	0	2	0	3	2	0	3	3
Verwoerd & Hunt, 2002	6	3	4	3	2	0	0	0
W. Y. C. Wang et al., 2016	0	0	3	0	0	0	0	0
W. Wang et al., 2019	1	11	0	4	9	1	6	2
Williams et al., 2013	2	0	0	3	3	3	9	2
Yu et al., 2013	1	2	2	0	0	2	0	0
Zhang et al., 2021	3	2	0	0	0	0	0	0
Total	126	140	34	99	77	68	114	76

Note: Legend: DO-ESR = Doing Engineering Cybersecurity Requirements; DO-DCS = Doing Designing Cybersecurity Solutions; DO-RDE = Doing Reviewing Cybersecurity Design; IM-SDA = Improve Standardizing Cybersecurity Activities; IM-ISD = Improving Cybersecurity; EN-SSA = Enable Supporting Cybersecurity Activities; MA-PMS = Planning and Managing Cybersecurity; and MA-MWO = Managing Stakeholders as DCCI first-order outcomes.

About the Authors

Angélica Pigola. PhD in Administration at University Nove de Julho (2023) and PhD candidate in Information Technology at EAESP Fundação Getúlio Vargas (2024). Master's in administration at University Nove de Julho (2021), Post-graduate in Marketing Administration at Fundação Armando Alvares Penteado (2000) and bachelor's degree in business administration at University Paulista (1995). Editor assistant of the International Journal of Innovation (IJI). Research focus on digital innovation technologies and information security. Corporate experience in Digital Transformation.

Priscila Rezende da Costa. Associate Director of Master and Doctoral Program in Administration at University Nove de Julho. She holds a PhD in Business Administration at the University of São Paulo, FEA USP (2012). Master's in business administration at University of São Paulo, FEA RP USP (2007). Currently, Director of Postgraduate Program in Administration at University Nove de Julho and major researcher of productivity scholarship, (PQ 2/ CNPq). Editor of the International Journal of Innovation (IJI) and Innovation & Management Review (IMR). Leader of the CNPq Research Group on Innovation Strategy, in research themes of company-university cooperation, dynamic capabilities, and internationalization of innovation.