NOVE DE JULHO UNIVERSITY
MASTER AND DOCTORAL PROGRAM IN ADMINISTRATION

ANGÉLICA PIGOLA

DEVELOPING AND INVESTING IN DYNAMIC CAPABILITIES INTO BUSINESS TO ENHANCE CYBERSECURITY INTELLIGENCE

This dissertation was carried out with the support of the Coordination for the Improvement of Higher Education Personnel - Brazil (CAPES) - Financing Code 001 (PROSUP), from 08/2021 to 10/2022. Subsequently, the CAPES scholarship for the Sandwich Doctorate Program Abroad (Aston University – UK) came into effect, from 11/2022 to 04/2023**.**

São Paulo

2023

Angélica Pigola

DEVELOPING AND INVESTING IN DYNAMIC CAPABILITIES INTO BUSINESS TO ENHANCE CYBERSECURITY INTELLIGENCE

DESENVOLVER E INVESTIR EM CAPACIDADES DINÂMICAS NOS NEGÓCIOS PARA MELHORAR A INTELIGÊNCIA DE SEGURANÇA CIBERNÉTICA

Tese apresentada ao Programa de Pós-Graduação em Administração da Universidade Nove de Julho – UNINOVE, como requisito parcial para obtenção do grau de **Doutor em Administração**.

Orientador: Prof. Dra. Priscila Rezende da Costa

Coorientador: Prof. Dr. Breno Nunes

São Paulo

2023

Pigola, Angélica.
Desenvolver e investir em capacidades dinâmicas nos negócios para melhorar a inteligência de segurança cibernética. / Angélica Pigola. 2023.
173 f.
Tese (Doutorado) - Universidade Nove de Julho - UNINOVE, São Paulo, 2023.
Orientador (a): Profª. Drª. Priscila Rezende da Costa.
1. segurança cibernética. 2. capacidades dinâmicas. 3. Inovação. 4. riscos virtuais. Recursos virtuais.
I. Costa, Priscila Rezende da. II. Título.

CDU 658

DESENVOLVER E INVESTIR EM CAPACIDADES DINÂMICAS NOS NEGÓCIOS PARA MELHORAR A INTELIGÊNCIA DE SEGURANÇA CIBERNÉTICA

ANGÉLICA PIGOLA

Tese apresentada ao Programa de Pós-Graduação em Administração - PPGA da Universidade Nove de Julho – UNINOVE, como requisito parcial para obtenção do título de Doutor em Administração, sendo a banca examinadora formada por:

_____

Prof. Dr. Gustavo Hermínio Salati Marcondes de Moraes – Universidade Estadual de Campinas – UNICAMP

_____

Prof. Dra. Gabriela Gonçalves Silveira Fiates – Universidade Federal de Santa Catarina – UFSC

_____

Profa. Dra. Cristiane Drebes Pedron – Universidade Nove de Julho – UNINOVE

_____

Prof. Dr. Fernando Antonio Ribeiro Serra – Universidade Nove de Julho – UNINOVE

São Paulo, 4 de Dezembro de 2023.

I dedicate this dissertation in memory of my beloved grandfather, João Pigola, who left me a legacy of wisdom and encouragement to study and improve my knowledge. Inspiring me, even if in dreams, to find myself again in something that would represent the best of me.

"God wants all mankind to be successful. The only way to do this, is to help individual people become better people and innovation is the key to unlocking more opportunities to do this always".
(Clayton M. Christensen)

First, I thank God and Jesus Christ for giving me the privilege of this academic journey, which represented a cycle of learning, reflection, and transformation. I have become more eager for new experiences, discoveries, and humble in the world's interactions. When we build our house on faith in God, the assurance that He always has a better place for us strengthens us.

I thank my beloved husband, Lucas, for the serenity that inspires me, the balance he teaches me, and the strength that infects and encourages me. Gratitude, love, and respect to you, who, since our first meeting, have helped me to be a more complete and happier human being. In our challenges and trials, we become stronger because our values and attitudes represent who we are. What I am is full of you and the immense love I feel for us together.

I am extremely grateful to my mother, Marli, and I thank her for her encouragement and presence. She serenely and lovingly supported me in my choices. Her complete dedication motivated me on my journey toward knowledge and academic growth.

Special attention to my advisor, Professor Dr. Priscila Rezende da Costa, who showed me academic focus, objectivity, and competence. She always guided me, protected me, and encouraged me to go further during this doctoral program. To all the professors, thank you for sharpening my critical-scientific and constructive thinking through effective collaboration to build my background as a researcher.

This research was supported by Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES, grant number 001.

RESUMO

Com os avanços e a utilização generalizada das tecnologias de informação e comunicação, os ataques cibernéticos estão a ter um impacto frequente e grave. As ameaças avançadas à segurança cibernética estão aumentando em setores como saúde, finanças, tecnologia, governo, varejo, transporte e muito mais. Os ataques cibernéticos também ameaçam a segurança de executivos, empresários e funcionários ou do público em geral com a perda de informações confidenciais; danos à reputação das empresas; problemas na tomada de decisões; défice monetário; perda de fiabilidade, etc. Portanto, é essencial avançar no sentido de analisar os recursos e capacidades relacionados com a segurança cibernética para identificar, prevenir e responder a tais violações. Nesta tese, o objetivo geral é apresentar uma visão para reduzir riscos e sensibilidades no ambiente virtual das empresas a partir da melhoria do processo de tomada de decisão ao investir no desenvolvimento de capacidades dinâmicas para proteção cibernética. Ela está estruturada em três estudos. O primeiro estudo foi uma metassíntese para identificar as principais capacidades de segurança cibernética em 47 estudos de caso. O segundo estudo é uma pesquisa empírica sem precedentes com 207 especialistas em segurança cibernética para confirmar a influência das capacidades dinâmicas na construção de inteligência em segurança da informação. E, por fim, o terceiro estudo, um experimento para avaliar a aprendizagem iterativa entre 26 indivíduos experientes e 83 não experientes em segurança da informação em relação a investimentos para desenvolvimento de capacidades dinâmicas em segurança da informação. Foi possível compreender os desafios que levam a atrasos na construção de capacidades que atendam cenários incertos e melhorem a previsibilidade de incidentes cibernéticos. Através de um modelo teórico sobre as dimensões que fomentam o desenvolvimento de capacidades de cibersegurança, de um estudo empírico para testar o modelo teórico e de uma experiência para analisar a eficácia da tomada de decisão sobre investimentos no desenvolvimento dessas capacidades, conclui-se que potenciais atrasos na a construção de capacidades de cibersegurança para enfrentar cenários incertos, melhorando a previsibilidade dos incidentes online, está diretamente ligada à invisibilidade dos riscos cibernéticos e ao conhecimento necessário para os compreender. Contudo, o aspecto mais positivo destas descobertas baseia-se na possibilidade efetiva de aprendizagem sobre como investir em capacidades de segurança cibernética para aqueles que desejam melhorar a postura organizacional em segurança da informação. Esta tese traz uma contribuição inédita para o cenário brasileiro, pois permite que as empresas inovem suas capacidades e processos de gestão de recursos para possibilitar maior segurança cibernética e reduzir os impactos de potenciais ataques virtuais, com probabilidade de erradicar vulnerabilidades. As abordagens metodológicas desenvolvidas também podem ser aplicadas a qualquer contexto, mediante adaptações apropriadas.

Palavras-chave: segurança cibernética, capacidades dinâmicas, inovação, riscos virtuais, recursos virtuais.

ABSTRACT

With advances and outspread usage of information and communication technologies, cyberattacks are growing into frequent and serious impact. Advanced threats in cybersecurity are on the rise in industries such as healthcare, finance, technology, government, retail, transportation, and more. Cyberattacks also threaten the security of executives, entrepreneurs and employees or the general public with the loss of confidential information; damage to the reputation of companies; trouble in decision-making; monetary deficit; loss of reliability etc. Therefore, it is essential to move towards analyzing cybersecurity-related resources and capabilities to identify, prevent and respond to such breaches. In this dissertation, the general objective is to present a vision to reduce risks and sensitivities in the virtual environment of companies from the improvement of the decision-making process on investing in the development of dynamic capabilities for cybernetic protection. It is structured in three studies. The first study was a meta-synthesis to identify key cybersecurity capabilities across 47 case studies. The second study is an unprecedented empirical survey of 207 cybersecurity experts to confirm the influence of dynamic capabilities on building intelligence in information security. And finally, the third study, an experiment to evaluate iterative learning among 26 experienced and 83 non-experienced individuals in information security in relation to investments for dynamic capabilities development in information security. It was possible to understand the challenges that lead to delays in building capabilities that meet uncertain scenarios and improve the predictability of cyber incidents. Through a theoretical model on the dimensions that foster the development of cybersecurity capabilities, an empirical study to test the theoretical model and an experiment to analyze the effectiveness of decision-making on investments in the development of these capabilities, it is concluded that potential delays in building cybersecurity capabilities to address uncertain scenarios by improving the predictability of online incidents is directly linked to the invisibility of cyber risks and the knowledge required to understand them. However, the most positive aspect of these findings is based on the effective possibility of learning on how to invest in cybersecurity capabilities for those who wish to improve the organizational posture in information security. This dissertation brings an unprecedented contribution to the Brazilian scenario, as it allows companies to innovate their capabilities and resource management processes to enable greater cybersecurity and reduce the impacts of potential virtual attacks, with the probability of eradicating vulnerabilities. The developed methodological approaches can also be applied to any context under appropriate adaptations.

Keywords: cybersecurity, dynamic capabilities, innovation, virtual risks, virtual resources

SUMMARY

LIST OF ILLUSTRATIONS

LIST OF TABLES

LIST OF ABREVIATIONS AND ACRONYMS

ACFE	The Association of Certified Fraud Examiners
AVE	Average Variance Extracted
BSIMM	Building Security in Maturity Model
CC	Cybersecurity Capabilities
CC_D	Cybersecurity Capabilities Doing
CC_E	Cybersecurity Capabilities Enabling
CC_I	Cybersecurity Capabilities Improving
CI	Cybersecurity Intelligence
CMMI	Capability Maturity Model Integration
DC	Dynamic Capabilities
DCCI	Dynamic Capabilities in Cybersecurity Intelligence
DCS	Designing Cybersecurity Solutions
COI	Cyber Occurrence Incident
ECR	Engineering Cybersecurity Requirements
EFA	Exploratory Factor Analysis
IMC	Improving Cybersecurity
ICT	Information and Communication Technologies
EPTD	Expected Percentage of True Differences
FDI	Factor Determinacy Index
IS	Information Systems
KMO	Kaiser-Meyer-Olkin
MAS	Managing Stakeholders
NIC	Innovations in cybersecurity
OCC	Organizational Cybersecurity Changes
OCP	Organizational Cybersecurity Performance
Pl	Profit Losses
Pe	Profit Earnings
PMC	Planning & Managing Cybersecurity
RCD	Reviewing Cybersecurity Design
RP	Percentage of profits invested in CC
SA	Systems Affected
SAD	Systems Affected and Detected
SNR	No Risk Systems
SPA	Supporting Cybersecurity Activities
STA	Standardizing Cybersecurity Activities
S_R	Sensitivity Ratio
SR	Systems at Risk

1 INTRODUCTION

Cyberattacks pose an ongoing threat as they are increasingly sophisticated. Companies seek to develop and deploy innovative technologies that will inadvertently bring into them new and shrewd vulnerabilities to users. Some years ago, cybersecurity was a question of “if” a company would be affected or compromised, but currently, it is a matter of “when” and “at what level” (D’Arcy et al., 2020; Jalali et al., 2019; Kour & Karim, 2020).

Critical cyberattacks and data breaches that affected firms worldwide demonstrate how relevant it is for firms that needs to be vigilant to effectively act and protect their assets against virtual risks (Pigola & da Costa, 2023). This concern is relevant because when firms do not react against cybersecurity transformation (i.e., adapted information technologies to deal with network challenges or to cope with post-pandemic effects), the data breach can be remarkable. Recent research demonstrated that in 2021, data breach was $5.01 million, being 20 percent more than the global overall average (IBM Security, 2021). Additionally, cyberattacks may produce irreparable harm to firms in the form of financial impact (Cavusoglu et al., 2004), corporate liability (Chellappa & Pavlou, 2002), failed competitive position, and loss of reputation (Crossler et al., 2013; Jalali & Kaiser, 2018).

As digital data grows in value and size, this cyber risk landscape increases the scale of privacy and digital protection concerns. Therefore, executives, entrepreneurs, and IT specialists must improve their approach to developing their capabilities and innovations aimed at cyber protection. For example, in Brazil, the National Council for Scientific and Technological Development (CNPq), the Minister of Health (ConectaSUS), and the Superior Court of Justice (STJ) suffered cyberattacks, losing part of their data and harming society. Brazil is the world's second most vulnerable country to cyberattacks (Forbes, 2023). This scenario emphasizes the relevance of investing and developing cybersecurity capabilities in any industry.

Interventions to build capabilities in cybersecurity and associated innovations make it possible to (1) manage uncertainty in resource availability (net revenue, talent availability, self-hosting, in-house systems development, IT policies, cybersecurity operations outsourcing, population data affecting business geographic, and data interactions); (2) detect external pressures (exploitation of successful criminal cyber events, loss of public reputation, threat of public or media backlash, regulation, audits);

(3) apprehension about complexity (managing multiple devices used together, employees bringing their own devices into the workplace, devices under regulation); and (4) promote internal alignment of stakeholders (when there is no single decision-making point, threat of regulatory fines, high turnover at the board level, growing executive awareness to give institutional power, acquisition process of dubious origin, direct experience with cyber crisis, ability to articulate damages, or design systems aligned with security policy) and (5) understanding criminal cyber activity [(financial, ideological, or related to terrorism to induce fear or cause delays in industry); (Jalali & Kaiser, 2018)].

Being prepared and proactively engaged in building dynamic capabilities in cybersecurity is higher cost-effective than more reactive approach when cyberattacks have already occurred (Adams & Makramalla, 2015; Benz & Chatterjee, 2020; Kwon & Johnson, 2014). While several firms are conscious of the importance of cybersecurity, a large part of Brazilian small and medium businesses remain out of date on the main cybersecurity requirements and resources to protect them from hackers (Benz & Chatterjee, 2020; Kabanda et al., 2018).

In this vein, this dissertation conceptualizes dynamic capabilities in cybersecurity as processes and abilities to identify, mobilize, and renewal resources against cyber risks. Additionally, individuals' proactive and reactive investment decisions in cybersecurity capabilities and associated innovation have received little attention, especially regarding cyber threats, misconceptions, and uncertainties about delays in realizing the earnings of these capabilities in real life (Catota et al., 2019; Dhillon et al., 2021). The general objective is to demonstrate that cybersecurity capabilities are positively associated with cyber intelligence creation to mitigate risks in information security. They also foster a strong cybersecurity posture in business improving the predictability of cyber uncertainties. And advancements in appropriate investments in cybersecurity capabilities can be learnt iteratively.

While individuals decision-making biases appear in a huge range in cybersecurity (Jalali et al., 2019; Rodgers et al., 2020; Rosoff et al., 2013), this dissertation focuses on providing the state of the art about dynamic capabilities in cybersecurity. In literature, the concepts of dynamic capabilities (Eisenhardt & Martin, 2000; Helfat et al., 2009; Teece et al., 1997), disruptive innovations (Christensen, 1997), and information systems security (Baskerville, 1989; Dhillon & Backhouse, 2001; Siponen & Vance, 2010) are interchangeable. Therefore, this dissertation also presents a redefinition of the term 'capacity' as a highly efficient organizational intangible resource to express problems and

solution space. In addition, it used historical literature (Dhillon et al., 2021; Dhillon & Backhouse, 2001) regarding the usefulness of evaluating security as a "risk analysis rooted in the functionalist paradigm". And understanding the capacity of cybersecurity as an efficient organizational resource is related to technical and social aspects of cyberattack detection, vulnerability management, and systematized security design data protection adapted to specific contexts.

Considering these challenges related to the impact of cybersecurity capabilities development and investments in business, the main research question posited in this dissertation is *at which level do cybersecurity capabilities development and investments affect cybersecurity intelligence in business*. To answer this question, objectives are in the next section, theoretical foundation is presented in section 1.2 and main contributions in section 1.3.

1.1 OBJECTIVES

1.1.1 Principal Objectives

Demonstrating that cybersecurity capabilities are paramount in cyber risks mitigation, cyber uncertainties reduction, and cyber innovations. The development of these capabilities directly impacts cybersecurity intelligence, and the investments can be learnt iteratively.

1.1.2 Specific Objectives

Considering the challenges inherent in cyber uncertainties and delays in cybersecurity capabilities development to virtual protection, this study specifically pursues:

- Understanding the scientific state of the art about capabilities in cybersecurity.
- Demonstrate the impact of cybersecurity capabilities in cybersecurity intelligence.
- Demonstrate differences in learning iteratively on how to invest in cybersecurity capabilities development for cybernetic protection between experienced and inexperienced groups.

- Understand whether the processes to invest in cybersecurity capabilities can be learned iteratively.

1.2 THEORETICAL FOUNDATIONS

The strategic management and organizational science literature highlight that discrepancies in firms' dynamic capabilities and resource configurations explain much of firms' performance heterogeneity (J. Barney, 1991; Grant, 1996; Helfat et al., 2009; Peteraf, 1993). However, an adequate reconfiguration of such capabilities and resources is a complex challenge not successfully achievable to all businesses (Dierickx & Cool, 1989; Eggers & Kaplan, 2009; Zollo & Winter, 2002). Likewise, cybersecurity feature composition is also closely linked to business performance, and some authors (Cavusoglu et al., 2015) show that there are huge variations in these feature configurations from firm to firm.

Academic literature has focused on the relationships between dynamic capabilities, decision-making, and organizational evolution in the cybernetic context (Shamim et al., 2019; Singh & Del Giudice, 2019; Wamba et al., 2017). The influence of dynamic capabilities fully mediates the effect of innovations (Mikalef et al., 2019) and influences effective investments in technologies (Adomavicius et al., 2008) and information security management (Bose & Luo, 2014; X. Li, 2021), which are themes of interest in business and academic circles (Bag et al., 2020).

In searching for potentially better intelligent capabilities to respond to contingent situations (Chatfield & Reddick, 2019), firms should innovate and strategically leverage cybersecurity posture developing their cybersecurity capabilities which will enable them to reach cyber resilience contributing to a long-term of competitiveness. (Kosutic & Pigni, 2022).

Recently, the authors Kosutic and Pigni (2022) defined cybersecurity posture as an organization's ability to build processes for developing cybersecurity capabilities and technological capabilities for new products. This allow firms to create differentiation and opportunities in revenues. The authors also understand that the competitive advantage achieved from developing cybersecurity capabilities derive from (1) the ability to protect digital assets and strategic intellectual property by being effective in digital protection and (2) the ability to bolster competitive advantage by improving product development through innovations in virtual protection.

While the growing body of cybersecurity literature discusses these questions to some extent, this study seeks to address the challenges of cybersecurity capability development in businesses. This study reviews this topic under two aspects of complexity: cyberattack uncertainty (Krutilla et al., 2021) and delays in investing and developing capabilities for cybersecurity (Jalali et al., 2019).

The first aspect is unpredictable cyber incidents, risks, and associated investments, evident in conventional theories of decision-making. The trade-off between protection return and risk is solved by risk-return combinative calculation (March & Shapira, 1987). However, the cyber risks, system performance, and costs of cybersecurity are all dubious, and few rational decision makers see security investments as an opportunity to reduce costs for the enterprise (Krutilla et al., 2021; Moore et al., 2015). Consequently, regarding allocating resources, the challenges to measure benefits and costs in cybersecurity investments obscure the perception and understanding of decision makers (D. S. Chai & Dirani, 2018).

Other challenges include the lack of effective metrics and historical data related to cyber incidents (Butler, 2002; van Haastrecht et al., 2021), in addition to weak knowledge in extent uncertainties, complexity, and predictability of future events (Komljenovic et al., 2016). According to Butler (2002), individuals use their own judgment, experience, and knowledge in decision-making about cyber events (Butler, 2002).

Risk perceptions are also associated with the cybersecurity triad: users, system, and usability. Users are characterized as experts (experienced) and nonexperts (not experienced) and have different characteristics that affect the use of systems (Rahman et al., 2021). Thus, a professional's organizational environment associated with information systems and individual characteristics drives his or her perception (Butler, 2002; Sawyer & Hancock, 2018; Straub & Welke, 1998). Some authors, shows that individuals lack strong intuition regarding high-consequence and low-probability in cyberattacks (Sawyer & Hancock, 2018). As an example, the more clearly an object can be seen, the closer it appears (Tversky & Kahneman, 2013). According to Jalali et al. (2019), if visibility is meager, people tend to undervalue the distance of an object as of them (Jalali et al., 2019).

The severity of cyber threats and their uncertain nature, combined with constant changes in technology implementation that may cause new vulnerabilities, make the decisions highly difficult in resources allocation such as investing in capabilities and innovations (S. Chai et al., 2011; Krutilla et al., 2021). Academic literature indicates that

investments in cybersecurity are associated with a reduction in the cost of capital but not a reduction in operating costs, as expected in the case of investments in information technology (Havakhor et al., 2020). The growing presence of virtual threats has resulted in technical defenses concentration neglecting appropriate investments in managing cybersecurity (Gordon & Loeb, 2002; Wirth, 2017).

According to some authors (Jalali et al., 2019; Madnick et al., 2017), if a firm does not experience any cyberattack, there is no motivation to allocate resources in prevention. Thus, individuals often do not adequately consider cyber events, therefore there is no surprise related to the significant gaps between individuals' perceptions and actual state of cybersecurity in an organizational scenario (Madnick et al., 2017). As a consequence, there is an underestimation about how often virtual incidents can occur and the time taking in developing cybersecurity capabilities to active detect, prevent, and respond to a cyberattack or data breach incident (Jalali et al., 2019).

Another aspect is the delays in the development of capabilities for cybersecurity that include interconnected components of web, among which the lags in emerging technologies increase the complexity of understanding the events and innovations necessary for virtual protection (Jalali & Kaiser, 2018). Troubleshooting methods are commonly used and are often aimed solely at remediating cyber events (Mihoubi et al., 2021; Sterman, 2001). Lags in building cybersecurity capabilities and enforcing decisions about innovations and the effects create instability and increase pressure to shorten the time span for appropriate corrective actions. Thus, this scenario leads to ineffective decision-making about cybersecurity posture and solvable paths.

These delays in developing capabilities for cybersecurity generate inadequate feedback loops between causes and effects, increasing the misunderstanding of scenarios that are difficult to predict (Repenning, 2002). According to some authors (Baghaei Lakeh & Ghaffarzadegan, 2016; Gonzalez et al., 2017), even experienced individuals have been demonstrated weak decision-making under such conditions. These experienced individuals may also believe that they understand cyber impacts much more than inexperienced individuals. However, the propensity to develop these type of capabilities combine with the daily hands-on create an observable set of activities that demand tasks and actions without bias about risks and information technologies (Carlton et al., 2019). Thus, organizations have considered investing and developing cybersecurity capabilities to encourage protection-motivated processes and organizational cybersecurity posture (Jalali et al., 2019; Johnston et al., 2016; Posey et al., 2017).

In sum, firms are not totally aware of these impacts of delays in developing cybersecurity capability, and they will fall into the short-term trap (aligned with the paradox of productivity and benefits of information technology investments). Many firms do not recover adequately and remain vulnerable to cyberattacks because cyber protection is also human-centered, so all sociotechnical aspects cannot be neglected (Dhillon et al., 2021; Rahman et al., 2021; van Haastrecht et al., 2021).

1.3 MAIN CONTRIBUTIONS

Dynamic capabilities theory in cybersecurity intelligence is inevitable considering that the cybersecurity phenomena embrace sociotechnical aspects. Building from a theorization to create an instrument to measure the impact of dynamic capabilities in cybersecurity intelligence, this dissertation contributes evidencing that the technical aspects are more impactful to build cybersecurity intelligence than managerial ones. This is relevant in terms of abilities to face a complex cybersecurity environment and improve appropriate decision-making about resources allocation to build identifiable and stable processes characterized as repeatable routines of investments in capabilities against cyber threats.

Additionally, the findings contributes revealing that the iterative learning process is a tacit option to firms bring attention to a stronger cybersecurity posture reinforcing capabilities toward precise organizational change including new or modified ways of operating according to different systemic scenarios under cyber threats. It is extremely positive, because this dissertation also shows that to learn about investments in cybersecurity capabilities is less complex than supposed to. However, it demystified that experienced individuals are ready to face cybersecurity challenges demonstrating that a continuous process of learning is a mandatory strategic in business when the subject is cybersecurity.

In sum, this dissertation contributes in several ways: (1) by presenting new perspectives for cybersecurity capabilities to enhance information security posture; (2) by exploring the response of individuals to decision-making in investing in cybersecurity capability development while considering the uncertainties of cyber risks; (3) measuring the iterative learning aftermath on proactive decision-making; (4) applying a new validity approach to cyber investments; and (5) from a systems approach, seeking to improve online protection using dynamic capabilities modeling.

1.4 PARADICMATIC STRUCTURE OF THE DISSERTATION

We explored dynamic capability development for cybersecurity intelligence based on theoretical and practical perspectives to answer the research questions across the studies. We employed a functionalist paradigm (Burrell & Morgan, 2017) to develop the studies and construct frameworks to enhance the science of dynamic capabilities in cybersecurity. This dissertation emphasizes the different theories that helped to conduct three studies for data gathering, analysis, findings, and more detailed in the following sections. Therefore, this study presents paradigmatic assumptions as the scientific foundation.

1.4.1 Ontological, Epistemological, and Axiological Assumptions

Research in the functionalist paradigm consider rational explanations and sets of recommendations within the current structures. Functionalist theories are often generalized to other contexts. The mainstream is that results can be applied universally by providing correctly implementation and monitoring (Kelemen & Rumens, 2008; Saunders et al., 2019). In this paradigmatic approach, ontology refers to presumptions about the nature of reality (Burrell & Morgan, 2017). Ontological assumptions shape how a researcher sees and studies a phenomenon. Ontology determines how a researcher describes the world, and thus, choose what to investigate in a research (Saunders et al., 2019).

Based on different theoretical foundations of social science (Burrell & Morgan, 2017; Hall, 2013; Maxwell, 2012; Saunders et al., 2019), this dissertation is developed as of ontological pragmatism and realism approach assuming organizational inference about the nature of facts. According to Maxwell (2012),

> The realist approach to validity also entails that a valid description, explanation, or interpretation must not only be supported by evidence, but also address plausible alternative descriptions, explanations, or interpretations of the phenomenon about which the claim is made. It is consistent with a regular view of causality as inherently general, dealing mainly with types of validity threats, rather than emphasizing the ways a specific conclusion might be wrong in a given study (p. 159).

The pragmatism approach follows Dewey's philosophical roots grounded in transactional realism (Biesta, 2010), moving away from the traditional dualism of

subjectivity and objectivity. This approach suggests that the world and mind are constantly interacting through transactions. According to Hall (2013),

> These transactions constitute an adjustive process whereby individuals actively engage, transform, or change the environment. These transactional experiences also produce knowledge that can continuously reconstruct reality. From a transactional realist perspective, the environment is not fixed, but in flux. This constant change presents situations that require adaptive behaviors from individuals, which is why Dewey argues inquiry is critical to managing this uncertainty (p.17).

Pragmatism integrates the natural sciences, and the social reality is external. It means, ontologically, pragmatism encompasses realism. It considers social entities like physical entities of the natural world. Thus, social entities exist independently of how individuals think, label or even be aware about them (Saunders et al., 2019).

Epistemology refers to knowledge. What constitutes valid, legitimate, or acceptable. And how it is communicated to others (Burrell & Morgan, 2017). Epistemologically, this dissertation pursues to uncover 'the truth' about the world through measurable and observable facts from which generalizations can be sketched about the reality (Saunders et al., 2019). Building upon a postpositivist perspective, which is an epistemological position that incorporates knowledge rejected by positivism as unscientific (Fox, 2008), this dissertation considers additional nuances of evidence emerged from the findings.

Although academic research rarely explores axiology, it does highlight the role of values and ethics. One of the key axiological alternatives faced in research is the extent to which the researcher's values and beliefs positively impact the research. Since social actors and social entities exist independently, this dissertation strives to remain free of the researcher's values or beliefs that could potentially bias the results. Thus, we proceeded with the rigorous scientific research process detached from any values and beliefs.

This dissertation also includes a determinist view, which regards individuals and activities as completely determined by the 'environment' or scenario in which they are located (Burrell & Morgan, 2017). Its reasoning is deductive occurring when conclusions are logically derived from theory premises. And they are true when all premises are also true (Ketokivi & Mantere, 2010; Saunders et al., 2019). In other words, the dissertation starts reading academic literature followed by research strategies designed to test the existing theories through a deductive approach.

Building upon this paradigmatic approach, all studies respect the criteria for judging the quality and validity suggested by Jahja (2017) for postpositivist approach in

ensuring (1) credibility; (2) transferability; (3) dependability, and (4) confirmability of findings (Jahja, 2017). According to Jahja (2007), "credibility is the "truth" of the findings, as viewed through the eyes of those being observed or interviewed and within the context in which the research is performed. Transferability is the extent to which findings can be transferred to other settings (similar contexts). Dependability is the extent to which the research produces similar or consistent findings if conducted as described. Confirmability occurs when the researcher needs to provide evidence that corroborates the findings. The subsequent chapters present the three studies that compose the main arguments of this dissertation" (p. 1)

1.5 DISSERTATION FRAMEWORK

The inherent aspects of capabilities associated with information security issues into firms and their associated unpredictability is the main concern of this dissertation justifying the adoption of mixed methods to support the logic of the central research question. Some authors (Velde et al., 2004) argue that the research strategy based on the sequential or simultaneous use of mixed methods is ideal for better interpreting and understanding an investigated reality. This methodological configuration is also recommended for the creation and subsequent validation of a theory or model (Morse, 2010). This mixed methods research was disseminated with the publication of the Handbook of Mixed Methods in the Social and Behavior Sciences by Tashakkori and Teddlie (2010) and detailed in a typology of mixed methods by Creswell and Clark (2018). More recently, Da Costa et al. (2019) presented an alternative structure proposition for PhD dissertation from multiple studies using these perspectives combined (Creswell & Clark, 2018; Da Costa et al., 2019; Tashakkori & Teddlie, 2010).

Following the suggestion proposed by Da Costa et al. (2019), this dissertation is what in fact particularizes and gives originality to scientific research in doctoral studies, assuming a structure of multiple studies, which can be adopted when the researcher is faced with the need to carry out and integrate different types of studies to answer the research problem (Da Costa et al., 2019). Thus, a theoretical study (meta-synthesis) and empirical studies (survey and experiment) answer the central research question giving originality to the findings. Table 1 presents the methodological matrix considering these perspectives.

Table 1. Methodological Matrix

MAIN RESEACH QUESTION **At which level do cybersecurity capabilities development and investments affect cybersecurity intelligence in business?**						
MAIN GOAL Demonstrating that cybersecurity capabilities are paramount in cyber risks mitigation, cyber uncertainties reduction, and cyber innovations. The development of these capabilities directly impacts cybersecurity intelligence, and the investments can be learnt iteratively.						
PARADIGM Functionalist = Ontology: Realism and Pragmatism | Epistemology: Postpositivist | Axiology: Objectivist | Human Nature: Determinist | Methodology: Multi-Methods						
JUSTIFICATION OF DISTINCTION			**JUSTIFICATION OF INTERDEPENDENCE**			
Study Title	**Secondary Research Questions**	**Objective**	**Sequential or simultaneous research**	**Single or mixed method in field stages**	**Data collection procedures**	**Data analysis procedures**
STUDY 1 Dynamics Capabilities in Cybersecurity Intelligence: A Meta-Synthesis to Enhance Protection Against Cyber Threats	What is an appropriate representation of dynamic capabilities in cybersecurity that build firm's cybersecurity intelligence?	Understanding the scientific framework about capabilities in cybersecurity.	Sequential Theoretical	Meta-Synthesis	Searching in Web of Science, Scopus, and AIS e-library	Coding structure of capabilities developed through Atlas.ti software from 47 case studies
STUDY 2 Dynamic Capabilities in Cybersecurity: Empirical Evidence to Enhance Management Against Cyber threats	Do dynamic capabilities in cybersecurity develop cybersecurity intelligence?	Demonstrate the impact of dynamic capabilities in cybersecurity to increase cybersecurity intelligence	Sequential Empirical	Regression Models	Survey questionnaire	Empirical data analysis from 207 cybersecurity experts in 22 countries
STUDY 3 Enhancing Cybersecurity Capabilities Investments: Evidence from an Experiment	Are there differences between experienced and inexperienced groups in investing in cybersecurity capability? Can the learning process in cybersecurity capabilities investments be achieved through a virtual iterative environment?	Understand whether the process to invest in cybersecurity capabilities can be learned iteratively.	Sequential Empirical	Experiment	Simulation of dynamic capabilities investments with experienced and inexperienced groups	Statistics and tests of normality and hypotheses of performance variation in leaning iteratively

Source. Adapted from Burrell and Morgan (2017) and Da Costa et al. (2019)

2 STUDY 1. DYNAMICS CAPABILITIES IN CYBERSECURITY INTELLIGENCE: A META-SYNTHESIS TO ENHANCE PROTECTION AGAINST CYBER THREATS

Advanced cybersecurity events are on the rise in industries such as healthcare, technology, retail, finance, transportation, government, among others. It is necessary to conduct analyses of cybersecurity-related resources and capabilities to build cybersecurity intelligence (CI). In this study, the general objective is to provide a Dynamic Capabilities in Cybersecurity Intelligence (DCCI) framework that helps to reduce risks of cyber violations and advance the development of systems and the life cycle of firms. Through a meta-synthesis, we analyzed in forty-seven empirical studies the application of cybersecurity capabilities to build CI combining theoretical and practical information security maturity models to understand the construction of structures that address uncertainty scenarios by improving the predictability of cyber incidents. The methodological approach supports any context, with the necessary adaptations. The results evidenced four second-order dimensions to build CI named doing, enabling, improving, and managing cybersecurity and eight first-order outcomes representing the DCCI framework. 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.

2.1 INTRODUCTION

Cyberattacks pose an ongoing threat as they are increasingly sophisticated, and companies seek to develop and deploy innovative technologies that require new and subtle capabilities for developers. Some years ago, information security was a matter of "if" a firms 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.Ik 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. Cybersecurity weaknesses may cause irreparable harm to a company in the form of corporate liability (Chellappa & Pavlou, 2002), and a poor competitive position due to loss of reputation (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 higher cost-effective than reactive approach about cybersecurity (Adams & Makramalla, 2015; Benz & Chatterjee, 2020; Kwon & Johnson, 2014). While several firms are already conscious about the relevance 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 cybersecurity posture through capability maturity models (Dube & Mohanty, 2020), we investigated under the perspective of dynamic capabilities theory the presence of technological, organizational, and managerial capabilities in 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 to specific threats. Adler (2013) was one of the first extended cybersecurity capability model into a dynamic performance built through an intuitive model-simulate-analyze methodology. Akinsanaya 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 (Akinsanya et al., 2019). Therefore, the purpose of our analysis and classification of some capabilities found in literature was to answer the research question about *what is an appropriate representation of dynamic capabilities in cybersecurity that build firm's cybersecurity intelligence?* We consider this approach valuable for firms' change and performance against cybersecurity weaknesses.

We provide a dynamic capabilities in cybersecurity intelligence (DCCI) model as a relevant approach investigating evidences of dynamic capabilities in 47 cases studies as of the Capability Maturity Model Integration (CMMI Institute, 2019) that enables firms to develop, assess, and improve resources in cybersecurity and as of 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 framework is closer to a realist approach from this sample of findings through meta-synthesis method. In other words, the objective of this study is to present an appropriate representation of technological, organizational, and managerial capabilities in cybersecurity to build firms' cybersecurity intelligence. For that purpose, we used two maturity models to serve as theoretical evidences, Capability Maturity Model Integration (CMMI Institute, 2019) and Building Security in Maturity Model (BSIMM, 2022) to develop the DCCI model identifying capabilities evidenced in real case studies, in an organized way, under the 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 general aim of this study is to provide that our DCCI framework supports the enhancement of cybersecurity intelligence. The findings reveal evidence in four second-order capabilities dimensions and eight first-order capabilities outcomes which represent our DCCI framework in firms' cybersecurity intelligence.

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 study 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.

2.2 THEORETICAL POSITIONING

According to some authors (Goode & Lacey, 2021; Leukfeldt et al., 2017; Spicer, 2019), cybercriminals may possess a different view of 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 study 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 as an 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 (J. B. 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. Thus, this validation offers scientific footing to the model becoming more implementable (Dube & Mohanty, 2020).

2.2.1 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 concerning organizational change in which DCs perform including new or modified ways of operating. And the second-order outcomes reflect organizational performance effects as a result of changes 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. Therefore, the authors provided theoretical foundations to the classification of dynamic capabilities across the case studies. For example, technological resources are associated with IT capabilities allowing firms to analyze their environments with more accuracy and speed on emerging opportunities. Studies have shown that IT capabilities possess higher value under high informational complexity (Mikalef et al., 2021) and fast-paced scenario (O.-K. Lee et al., 2015; Pavlou & El Sawy, 2006). Organizational and managerial resources, together, are concerned with how decisions-making processes influence DCs. The reasoning behind 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 evolutionary organizational fitness (Helfat & Winter, 2011).

IT capabilities serves as the vehicle on which such evolution can be enacted (Iyengar et al., 2015).

Providing a 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" (p. 461). These attributes purposely exclude both 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 attacker's capabilities, resources, motivations, and goals to assist firms in their decision-making processes to enhance cyber defense strategies (Kolini & Janczewski, 2022).

To organize the perspective of DCCI, we first took from 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), p. 215766]. 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 empirical 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).

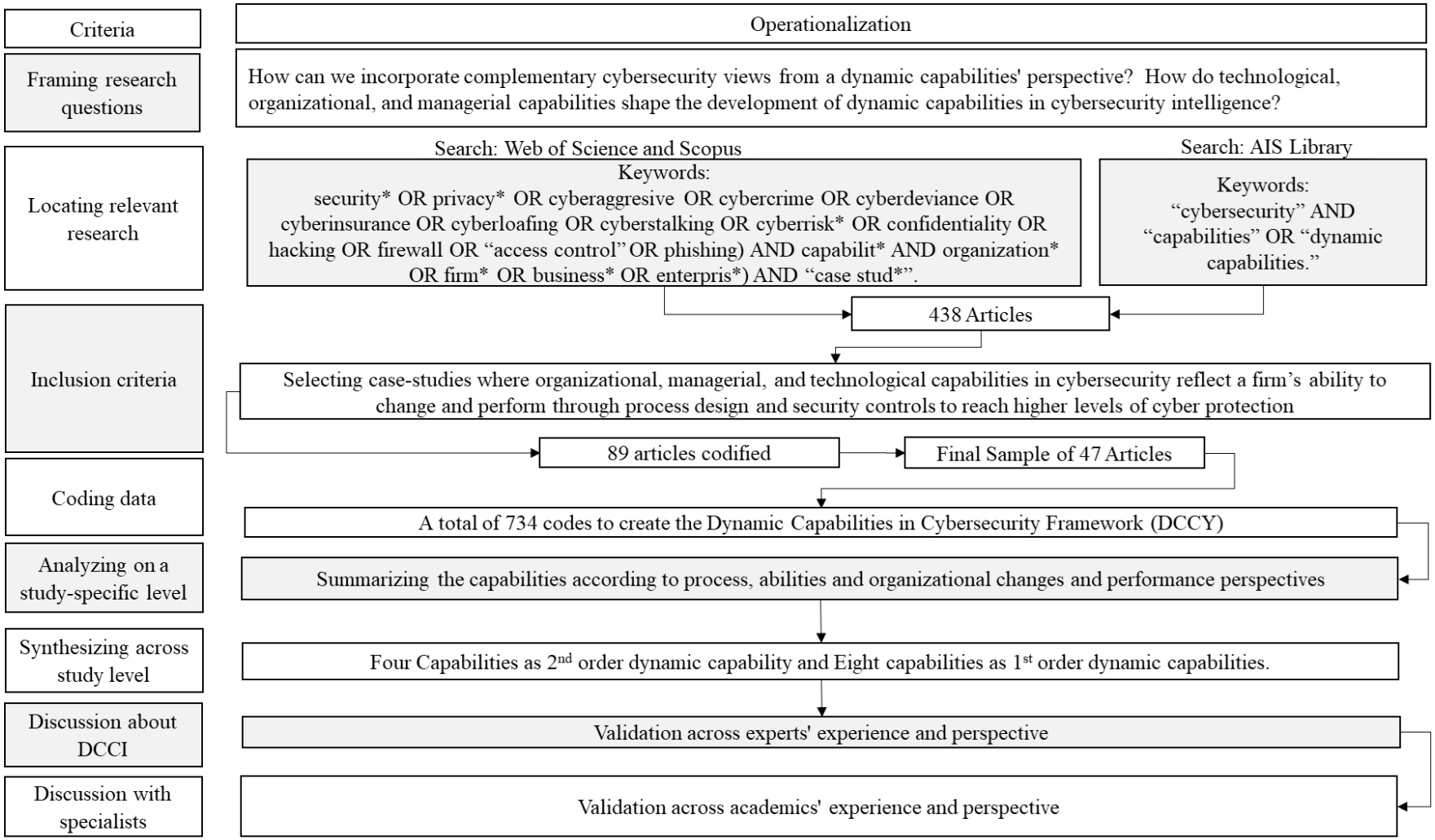
2.3 META-SYNTHESIS RESEARCH DESIGN

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-analysts have generated transparent rules on reporting the conduct of meta-analysis with replicability enhancing the product of a synthesis (Aytug et al., 2012; Carlson & Ji, 2011; Dalton & Dalton, 2008; Hoon, 2013).

Figure 1 shows a summary of methodological steps of this study and a description of the procedures, purpose and actions applied are shown in Table 2. 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). All the steps involved in this meta-synthesis are detailed in the following sections.

Figure 1. Methodological Steps of Meta-Synthesis



Source. Elaborated by author (2022)

Table 2. Meta-Synthesis Protocol

Steps in Meta-Synthesis	Analytical Description	Analytical Procedure	Outcome of each step
Framing research question	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	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 journals from IS areas, with the final sample of eighty-nine case studies to ensure reliability
Inclusion criteria	Precise inclusion and exclusion criteria applied and presented to determine which studies to include in terms of the method, theoretical foundations, research focus, initial research question, and quality	Developing and discussing an inclusion/exclusion criteria list.	Limiting eighty-nine case studies found in literature to a set of forty-seven case studies finally incorporated in the meta-synthesis; providing clear exclusion criteria to ensure validity, reliability, replicability.
Coding data	Carefully reading of full text of each 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 study-specific level	Identifying a sequencing of variables in each study to be the most influential in accounting for how capabilities change and perform in cybersecurity as DCs.	Study-specific causal	Identifying themes, patterns, core concepts and relationships in each study
Synthesizing across study level	Merging the study-specific into a meta-causal network. Concentrating the sequencing of variables at a cross-study 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.
Discussion about DCCI	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 literature on DCs	Clarification of the second-order dimensions of DCCI; arguing for their contribution to practice and theory
Discussion with specialists	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

Source. Adapted from Hoon (2013)

2.3.1 Step 1: Framing the Research Question

Starting with a conceptual framing of the topic, 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 *what is an appropriate representation of dynamic capabilities in cybersecurity that build firm's cybersecurity intelligence?* 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 questions was conducted by the authors and two additional specialists in cybersecurity.

A meta-synthesis takes advantage of a theoretically informed research question, well-specified, in contrast to the broader or conventional literature 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. In this study, 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.

2.3.2 Step 2: Locating Relevant Research

In this step, 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 the study of Dhillon et al. (2020), 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 eighty-one journals selected in the IS research field. The list of journals is provided in Appendix A. Proceedings, editorials, and books were excluded and a cross-checking of the articles regarding their methodological approach identified a sample of eighty-nine case studies published between January 1995 and March 2022, where the abstracts and keywords varied in content.

After reading, analyzing, and applying the inclusion and exclusion criteria previously defined and presented in the next section related to the content of each article, we search 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. 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 articles entail the increased scientific rigor resulting from a peer-reviewed publication process" (p. 531). 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 articles published in high-quality journals, excluding articles published in conference proceedings, and book chapters, as well as dissertations and unsubmitted or unpublished research studies.

2.3.3 Step 3: Inclusion and Exclusion Criteria

Determining and adopting the inclusion/exclusion criteria 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 questions, the criteria

are explained in Table 3. Following these predetermined criteria, only articles explicitly addressing the cybersecurity capabilities approach were considered. Given the meaning embedded in the term "capability" in this study 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 articles 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 assets, whilst external position concerns the market scenario 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 3. Inclusion and Exclusion Criteria

Criteria	Rationales	Reasons for Exclusion
Only Case Study	The criterion ensures that there is no difference between the research method the primary researchers claim to have used and the approach used. Excluded articles use, for example, illustrative examples to give an in-depth example of how a framework works or not to understand capabilities in cybersecurity. In addition, studies primary relying on quantitative data.	Illustrative study examples and publications out of the top list of journals created the by Science Citation Index Expanded (SCI-EXPANDED), Social Sciences Citation Index (SSCI) of Thomson-ISI Web of Science and AIS Journals list.
Articles initially framed in cybersecurity 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.
Refer to the processes of cybersecurity	Identify the studies on cybersecurity capabilities as a strong capacity to overcome cybersecurity challenges. This entails the inclusion of articles that provide a substantive contribution of cybersecurity capabilities in firm's change and performance.	Without focus on cybersecurity capabilities or its applications and development.
Focus on cybersecurity in the study's a priori goals, research question, and research interests	This criterion enables cybersecurity capability studies with a priori research question(s) or goal(s) in cybersecurity. Therefore, case studies should provide a primary focus on the technological, organizational, or managerial capabilities approach to explain changes in the cybersecurity scenario.	Cybersecurity perspective not included in the initial main research objective
Check quality	Quality of all studies checked. According to standards and guidelines (Eisenhardt, 1989; Yin, 2014), the studies are 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

Source: Adapted from Hoon (2013)

2.3.4 Step 4: Extracting and Coding Data

In this step, 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 guidelines of Gioia et al. (2013), this study seeks qualitative rigor and systematically transfers raw data into theoretical interpretations (Corley & Gioia, 2004; Gioia et al., 2013).

Each primary study was coded for the descriptive characteristics such as type of study 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 Miles and Huberman's (1994, p.64) 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]

→ [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 Atlasti 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 an example of coding process and Appendix D the synthesized structure of 734 codes of a network of DCCI capabilities.

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).

2.3.5 Step 5: Analyzing on a study-specific level.

The process of data analysis was 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 articles. 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).

2.3.6 Step 6: Synthesis of DCCI at a Cross-Study Level

From a study-specific level to a cross-study level analysis, this step merges the capabilities identified in each 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 D provides the synthesized structure of 734 codes of a network of 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.

2.3.7 Step 7: Discussion of Dynamic Capabilities in Cybersecurity Intelligence

As a result, 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 4). 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 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" (p. 5054). 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.

Table 4. 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).	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
		Transforming	*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.		

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.	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
		Seizing	*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.		
	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 Steininger 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

Note. Combinative descriptions based on case study findings, discussion sections.

Legend: OC= Organizational Change; OP = Organizational Performance; P = Processes; A = Abilities

Source: 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 & Moe, 2017; Bradford et al., 2014; Cahyani et al., 2017; Diaz et al., 2019; Goles et al., 2008; Goode & Lacey, 2021; Laamanen & Wallin, 2009; Magnuson et al., 2004; Mathrani & Lai, 2021; H. Naseer et al., 2021; Renwick & Gleasure, 2021; Seethamraju, 2015; Tan et al., 2016; W. Wang et al., 2019; Williams et al., 2013).

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).

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].

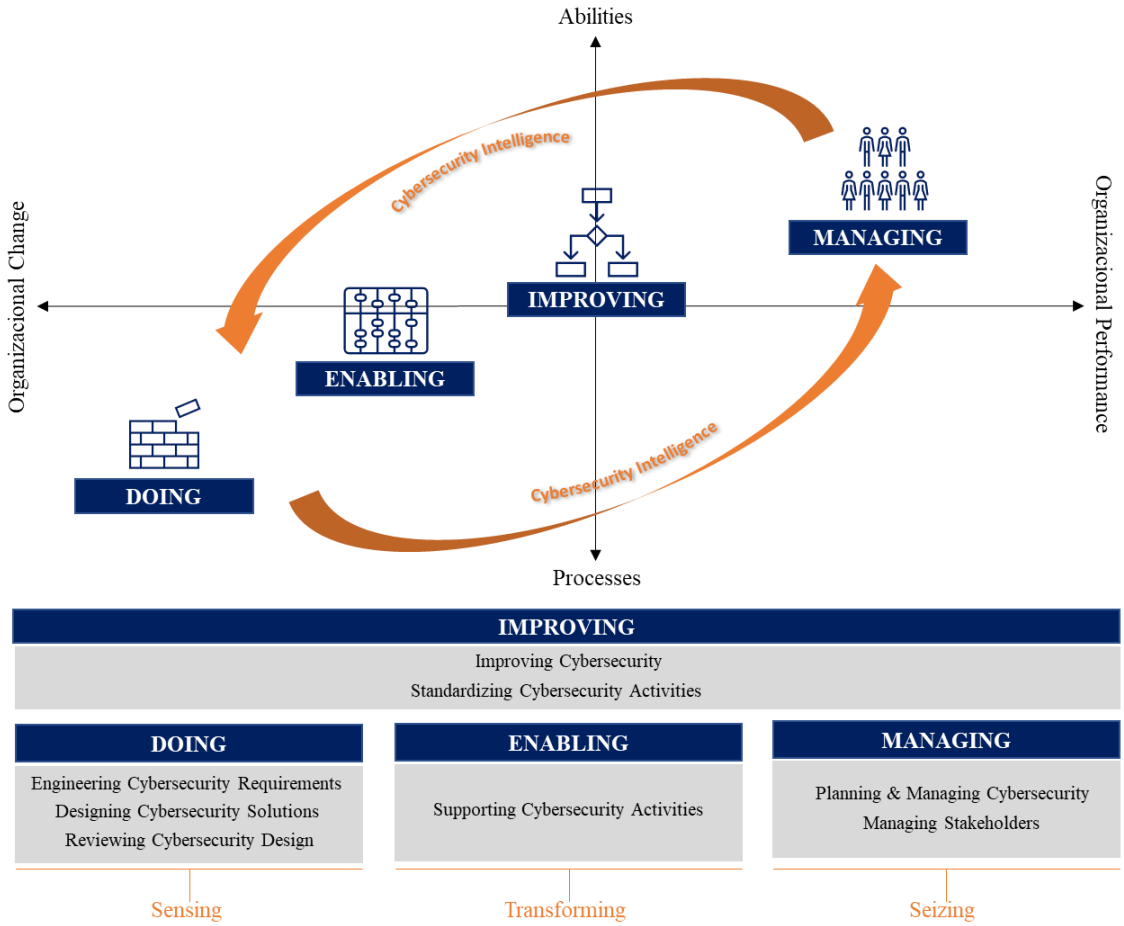
Given the sensitive nature of cybersecurity issues, only a dynamic multi-dimensional process (Williams et al., 2013) cannot be the way to fully resolve cyber threats, as the involvement of humans (mainly cybersecurity managers) is critical to investigating and confirming these threats, particularly when they are internal (H. Naseer et al., 2021). Therefore, understanding the processes and ability in the proposed DCCI framework (See Table 4) 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 2. DCCI Framework: Holistic View



Source. Elaborated by authors (2022)

2.3.8. Step 8. Discussion with specialists

The last step, according to the recommendation of Hoon (2013), 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. 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 articles 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 article 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. 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).

2.4 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 found in literature, 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 4 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 questions 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.

2.4.1 Theoretical Contribution

Our study 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 study addressed the research questions by developing the DCCI framework 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).

2.4.2 Managerial Implications

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.

2.4.3 Limitations and suggestions for future research

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; Seaman, 1999; van Heesch et al., 2012). 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 adoption.

*T*o 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., firms in different regions and industries) could be included.

To sum up, as this meta-synthesis demonstrates the versatility of DCCI in firms' change and performance, firms 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.

2.5 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

2.6 APPENDIX A. SOURCE TITLE RANKING

Source Title	**Number of Publications (n= 150)**
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
Administrative Sciences	1
African Journal of Information Systems	1
Applied Sciences-Basel	1
Business Information Review	1
BMC Medical Informatics and Decision Making	1
Computers & Industrial Engineering	1
Community College Journal of Research and Practice	1
Computers and Electronics in Agriculture	1
Computers in Human Behavior	1
Computers, Materials and Continua	1
Concurrency and Computation: Practice and Experience	1
Egyptian Informatics Journal	1
Electronic Markets	1
Electronics	1
Future Generation Computer Systems	1
IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems	1
IEEE Transactions on Computers	1
IEEE Transactions on Engineering Management	1
IEEE Transactions on Visualization and Computer Graphics	1
Government Information Quarterly	1

ISPRS International Journal of Geo-Information	1
Industrial Marketing Management	1
Information Management and Computer Security	1
Information and Computer Security	1
Information and Software Technology	1
Information Polity	1
International Business Review	1
International Journal of Accounting Information Systems	1
International Journal of Emerging Technologies in Learning	1
International Journal of Nursing Studies	1
International Journal of Information Technology and Management	1
Journal of Theoretical and Applied Eletronic Commerce Research	1
Journal of the American Medical Informatics Association : JAMIA	1
Journal of Business and Industrial Marketing	1
Journal of Automated Reasoning	1
Journal of Chinese Economic and Foreign Trade Studies	1
Journal of Information Science	1
Journal of Intelligent Information Systems	1
Journal of Intelligent Manufacturing	1
Journal of International Management	1
Journal of Parallel and Distributed Computing	1
Journal of Public Health Management and Practice	1
Journal of Supercomputing	1
Neural Computing and Applications	1
Organization Science	1
Policy and Internet	1
Scalable Computing	1
Scandinavian Journal of Information Systems	1
Science of the Total Environment	1
Sensors	1
Social Science Computer Review	1
Telecommunication Systems	1
Telematics and Informatics	1
Wireless Personal Communications	1
Work	1

Note. List ranking based on the initial sample (438 publications)

2.7 APPENDIX B. ARTICLES ANALYZED: INCLUSION AND EXCLUSION CRITERIA

ID	Authors	Title	Source title	Main variables under attention	Capability	Inclusion/ Exclusion	Empirical Context
1	(Er et al., 2022)	Trust-aware process design: the case of GoFood	Business Process Management Journal	Trust-aware process design (input, people, process, and output)	OM	0	GoFood Company, a food delivery company in Indonesia
2	(Humayun et al., 2022)	Security Threat and Vulnerability Assessment and Measurement in Secure Software Development,	Computers, Materials and Continua	Security Best Practices in system development life cycle	T	0	Organization XYZ
3	(Kapoor et al., 2021)	Ransomware detection, avoidance, and mitigation scheme: A review and future directions	Sustainability	Ransomware Defence (detection, avoidance, and mitigation)	T	0	The infamous Djvu Ransomware case
4	(H. Hsu et al., 2021)	Clinical informatics during the COVID-19 pandemic: Lessons learned and implications for emergency department and inpatient operations,	Journal of the American Medical Informatics Association : JAMIA	Telemedicine	OM	1	At NewYork Presbyterian, a nonprofit healthcare network
5	(W. Wu & Plakhtii, 2021)	E-Learning Based on Cloud Computing,	International Journal of Emerging Technologies in Learning	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)
6	(Rukanova et al., 2021)	Identifying the value of data analytics in the context of government supervision: Insights from the customs domain	Government Information Quarterly	Value of Data Analytics in Government Supervision	OM	2	PROFILE research project funded
7	(Stacey et al., 2021)	Emotional reactions and coping responses of employees to a cyber-attack: A case study	International Journal of Information Management	Emotional responses for cybersecurity	T	2	Global manufacturing company

8	(Al-Matari et al., 2021)	Adopting security maturity model to the organizations' capability model,	Egyptian Informatics Journal	Information Security Management Model	OM	0	Retirement organization and public telecommunication corporation in the Republic of Yemen.
9	(Zhang et al., 2021)	Interoperable multi-blockchain platform based on integrated REST APIs for reliable tourism management	Electronics	Multi-chain blockchain architecture to enhance the transaction processing capability	T	0	Hotel Booking Winding Tree and Hyperledger Fabric in the tourism industry
10	(Gong & Janssen, 2021)	Roles and Capabilities of Enterprise Architecture in Big Data Analytics Technology Adoption and Implementation	Journal of Theoretical and Applied Electronic Commerce Research	Big Data Analytics	TOM	0	Dutch Tax and Customs Administration in the Netherlands
11	(Goode & Lacey, 2021)	Exploiting organizational vulnerabilities as dark knowledge: conceptual development from organizational fraud cases	Journal of Knowledge Management	Dark Knowledge (ability to identify organizational weaknesses, vulnerabilities, and compromise points)	TOM	0	A large Asia-Pacific telecommunications provider
12	(Mathrani & Lai, 2021)	Big Data Analytic Framework for Organizational Leverage	APPLIED SCIENCES-BASEL	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).
13	(A. Naseer et al., 2021)	Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis	International Journal of Information Management	Real-time analytics Capability (complex event processing, decision automation, and on-demand and continuous data analysis)	TOM	0	Twenty cybersecurity experts interviews
14	(Renwick & Gleasure, 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	Privacy Attitudes (Privacy-related concepts, resources, and methods for blockchain technologies)	TOM	0	Monero, a cryptocurrency community

15	(R. Smith et al., 2021)	The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework	Computers & Security	Agile techniques into the Cyber Security domain of incident response	TOM	0	Protecting Industrial Control Systems
16	(Ahmed et al., 2021)	How can organizations develop situation awareness for incident response: A case study of management practice	Computers & Security	Situation Awareness in incident response	OM	0	Large multinational finance organization
17	(H. Naseer et al., 2021)	Demystifying analytical information processing capability: The case of cybersecurity incident response	Decision Support Systems	Information processing capability in cybersecurity incident response	TOM	0	Twenty-seven participants, drawn from three financial sector firms
18	(Hosseini et al., 2020)	Ripple effect modelling of supplier disruption: integrated Markov chain and dynamic Bayesian network approach	International Journal of Production Research	Vulnerability and Recoverability capabilities	T	1	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.
19	(Tigharsi et al., 2019)	The paradox of roots and wings: labor mobility between local firms and MNEs in North Africa	Journal of Knowledge Management	Labor Mobility	OM	2	12 employees in different industries
20	(Brous & Janssen, 2020)	Trusted decision-making: Data governance for creating trust in data science decision outcomes,	Administrative Sciences	Mature data governance capability	OM	0	A large European public organization projects in Road management and Electrical Grid Management
21	(Akinsanya et al., 2019)	Towards a maturity model for health-care cloud security (M2HCS),	Information and Computer Security	Health-care cloud security	TOM	0	Hospitals' cyber security internal processes
22	(Ghobakhloo & Fathi, 2019)	Corporate survival in Industry 4.0 era: the enabling role of lean-digitized manufacturing,	Journal of Manufacturing Technology Management	Hybrid lean-digitized manufacturing system	TOM	0	Small manufacturing firm
23	(Al-Matouq et al., 2020)	A Maturity Model for Secure Software Design: A Multivocal Study	IEEE Access	Secure Software Design Maturity Model	TOM	0	Two software organizations in Saudi Arabia

24	(Montealegre et al., 2019)	Understanding Ambidexterity: Managing Contradictory Tensions Between Exploration and Exploitation in the Evolution of Digital Infrastructure	Journal of the Association for Information Systems	Digital Infrastructure Ambidexterity	TOM	2	RE/MAX LLC, a global real estate franchise
25	(Diaz et al., 2019)	Self-service cybersecurity monitoring as enabler for DevSecops	IEEE Access	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.
26	(Johansson et al., 2019)	Smart and sustainable emaintenance: Capabilities for digitalization of maintenance	Sustainability	Assuring Information Security (Correctness, Confidentiality, Accessibility)	T	0	Digital railway maintenance development company and its main customer
27	(Q. Li et al., 2019)	A Framework for Big Data Governance to Advance RHINs: A Case Study of China	IEEE Access	Healthcare Big Data Governance Practices	TOM	0	Ten typical regional health information networks in China
28	(W. Wang et al., 2019)	Uncertain environment, dynamic innovation capabilities and innovation strategies: A case study on Qihoo 360	Computers in Human Behavior	Dynamic innovation capabilities and innovation strategies	TOM	0	Internet security industry
29	(Holen-Rabbersvik et al., 2018)	Barriers to exchanging healthcare information in inter-municipal healthcare services: A qualitative case study,	BMC Medical Informatics and Decision Making	Communication and Information Sharing	M	1	Inter-municipal healthcare services
30	(Abdul Molok et al., 2018)	A case analysis of securing organizations against information leakage through online social networking	International Journal of Information Management	Leakage Mitigation Capability	OM	0	Four Firms in Malaysia at various levels of maturity in relation to the security management of Online Social Networking
31	(Chatfield & Reddick, 2019)	Crowdsourced cybersecurity innovation: The case of the Pentagon's vulnerability reward program,	Information Polity	Crowdsources software bug detection	OM	0	Pentagon vulnerability reward program or bug bounty program
32	(D'Orazio & Choo, 2018)	Circumventing iOS security mechanisms for APT forensic investigations: A security taxonomy for cloud apps	Future Generation Computer Systems	Security Mechanisms in mobile platforms and apps	T	0	Eighteen popular iOS cloud apps

33	(Lu & Sinnott, 2018)	Semantic privacy-preserving framework for electronic health record linkage	Telematics and Informatics	Access control policy	T	0	Australasian Paediatric Endocrine Group and the Juvenile Diabetes Research Foundation
34	(Attili et al., 2018)	Understanding information privacy assimilation in its organizations using multi-site case studies,	Communications of the Association for Information Systems	Privacy Capabilities (Information Privacy and Privacy Assimilation)	TOM	0	Eighteen IT organizations in India and USA
35	(A. Hall et al., 2017)	Implementing monitoring technologies in care homes for people with dementia: A qualitative exploration using Normalization Process Theory,	International Journal of Nursing Studies	Implementation of monitoring technologies in care homes	M	1	Three dementia-specialist care homes in North-West England
36	(Dang-Pham et al., 2017)	Applications of social network analysis in behavioral information security research: Concepts and empirical analysis	Computers & Security	Behavioral information security	OM	1	A large organization in Vietnam
37	(Rehm et al., 2017)	Using Information Systems in Innovation Networks: Uncovering Network Resources	Journal of the Association for Information Systems	Networking Capabilities	OM	2	Cooperative research project called SmartNets partly funded by the European Commission
38	(Aoki & Wilhelm, 2017)	The Role of Ambidexterity in Managing Buyer-Supplier Relationships: The Toyota Case	Organization Science	Ambidexterity	OM	2	Toyota Motor Corporation
39	(Oguntala et al., 2017)	Systematic Analysis of Enterprise Perception towards Cloud Adoption in the African States: The Nigerian Perspective	African Journal of Information Systems	Poor adoption of cloud computing	OM	2	African Entreprise in Nigeria
40	(Ritchie et al., 2017)	A case study detailing key considerations for implementing a telehealth approach to office ergonomics,	Work	Telehealth-based ergonomics service delivery process	T	2	Alberta-based non-profit advocacy group
41	(C. Wu et al., 2017)	A NoSQL-SQL hybrid organization and management approach for real-time geospatial data: A case study of	ISPRS International Journal of Geo-Information	Geographic video surveillance	T	2	144 Hospitals listed in Taiwan Joint Commission on Hospital Accreditation

		public security video surveillance					
42	(Mani et al., 2017)	Mitigating Supply Chain Risk via Sustainability Using Big Data Analytics: Evidence from the Manufacturing Supply Chain	Sustainability	Big Data Analytics	TOM	2	Surat Milk Union Limited firm, Gujarat, India
43	(Bartnes & Moe, 2017)	Challenges in IT security preparedness exercises: A case study	Computers & Security	Security Incidents Preparedness	OM	0	Norwegian Distribution System Operators
44	(Cahyani et al., 2017)	Forensic data acquisition from cloud-of-things devices: windows Smartphones as a case study	Concurrency and Computation-Practice & Experience	Mobile Forensic Tool Capabilities	T	0	Windows phone (cloud-of-things device)
45	(Rashidi & Rezakhani, 2017)	A new approach to ranking attributes in attribute-based access control using decision fusion,	Neural Computing and Applications	Attribute based access control	T	0	Enterprises IT managers
46	(Tan et al., 2016)	Information and Knowledge Leakage in Supply Chain	Information Systems Frontiers	Knowledge and Information Leakage	OM	0	Five manufacturing companies in Malaysia
47	(W. Y. C. Wang et al., 2016)	How social media applications affect B2B communication and improve business performance in SMEs	Industrial Marketing Management	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
48	(Crandall & Allan, 2015)	Small states and big ideas: Estonia's battle for cybersecurity norms	Contemporary Security Policy	Estonia's Norm-building in cybersecurity	OM	1	Estonian government norms
49	(Krishnan & Vorobyov, 2015)	Enforcement of privacy requirements	Computers & Security	Access Control	T	1	E-voting Protocols
50	(Jin et al., 2015)	Formation of R&D alliances in the Chinese mobile telephony industry,	Journal of Chinese Economic and Foreign Trade Studies	International R&D alliances	OM	2	Chinese local firms in telecommunication industry
51	(Lei & Moon, 2015)	A Decision Support System for market-driven product positioning and design	Decision Support Systems	Decision Support System for market-driven product positioning and design	T	2	US automotive market data

52	(Seethamraju, 2015)	Adoption of Software as a Service (SaaS) Enterprise Resource Planning (ERP) Systems in Small and Medium Sized Enterprises (SMEs)	Information Systems Frontiers	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
53	(Blanco et al., 2015)	An architecture for automatically developing secure OLAP applications from models,	Information and Software Technology	Secure Data Warehouse repository	T	0	A Sales department
54	(Jiang & Okamoto, 2014)	National identity, ideological apparatus, or panopticon? A Case Study of the Chinese national search engine Jike,	Policy and Internet	China's national search engine.	OM	2	Jaike Company
55	(Patel et al., 2014)	Promoting food security and livelihoods for urban poor through the informal sector: a case study of street food vendors in Madurai, Tamil Nadu, India	Food Security	Food security Status	OM	2	Street food sector in Madura, India.
56	(Bradford et al., 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	End-to-end identity and Access management	TOM	0	Two large higher educational institutions
57	(Hughes & Chapel, 2013)	Connect, communicate, collaborate, and create: Implementing an enterprise-wide social collaboration platform at KPMG - Part two: Realizing value,	Business Information Review	Internal social collaboration platform called the Hub	OM	1	KPMG
58	(Piekkari et al., 2013)	Translation behavior: An exploratory study within a service multinational	International Business Review	Translation behavior	OM	2	Nordic Bank

59	(Yu et al., 2013)	Rule-based security capabilities matching for web services	Wireless Personal Communications	Web Service Policy Security Capabilities	TOM	0	Four security requirements cases on Web service
60	(Williams et al., 2013)	Information security governance practices in critical infrastructure organizations: A socio-technical and institutional logic perspective	Electronic Markets	Information Security Governance	OM	0	Fourteen Australian critical infrastructure organizations
61	(Corallo et al., 2012)	Inter-organizational knowledge integration in Collaborative NPD projects: evidence from the aerospace industry	Knowledge Management Research & Practice	Knowledge Protection (Human Resources Awareness, Legal Structure, Alliance Process)	OM	0	Two Italian aerospace firms
62	(Aissani et al., 2012)	Dynamic scheduling for multi-site companies: A decisional approach based on reinforcement multi-agent learning	Journal of Intelligent Manufacturing	Learning Capabilities	T	0	Multi-site companies supply chain planning
63	(Desouza, 2011)	Securing intellectual assets: integrating the knowledge and innovation dimensions	International Journal of Technology Management	Security Intellectual Mgmt (Source, Analytics, Interpretation, Action)	OM	1	Executives involved in security management programs in twenty-three firms
64	(Barletta et al., 2011)	Workflow and access control reloaded: A declarative specification framework for the automated analysis of web services,	Scalable Computing	Access Control in Web Services	T	0	e-business Banking Service and Digital Contract Signing in the e-government area
65	(Batra et al., 2010)	Balancing Agile and Structured Development Approaches to Successfully Manage Large Distributed Software Projects: A Case Study from the Cruise Line Industry	Communications of the Association for Information Systems	Agile methods and the traditional structured	OM	2	Cruise Line Industry
66	(Knoerich, 2010)	Gaining from the global ambitions of emerging economy enterprises: An analysis of the decision to sell a German firm to a Chinese acquirer	Journal of International Management	Cross-border acquisitions by companies	OM	2	Chinese acquisitions of German firms in the machinery and equipment industry

67	(Kumar et al., 2010)	A closed loop outsourcing decision model for developing effective manufacturing strategy	International Journal of Production Research	Sourcing Decisions	OM	2	US manufacturer of industrial thermal transfer bench-top printer
68	(Zhen et al., 2010)	A real-time simulation grid for collaborative virtual assembly of complex products,	International Journal of Computer Integrated Manufacturing	Collaborative virtual assembly scheme based on grid technology	T	2	A car-assembly workstation
69	(de Leusse et al., 2010)	Securing business operations in an SOA	Security and Communication Networks	Collaborative Engineering (policy enforcement, identity brokerage, access management and security governance)	TOM	0	Service Oriented Enterprise in Aerospace industry
70	(Chen et al., 2009)	Flexible authorization in dynamic e-business environments using an organization structure-based access control model,	International Journal of Computer Integrated Manufacturing	Secure Access Control	OM	0	An automobile component producer
71	(Laamanen & Wallin, 2009)	Cognitive dynamics of capability development paths	Journal of Management Studies	Capabilities Development	TOM	0	Three network security software firms
72	(Krogh et al., 2008)	Managing Online in Perpetual Perfect Storms: Insights from IndyMac Bank	MIS Quarterly Executive	IT-intensive mortgage bank	OM	2	IndyMac Bank
73	(Mathiassen & Pedersen, 2008)	Managing Uncertainty in Organic Development Projects	Communications of the Association for Information Systems	Management of uncertainty in organic systems development	OM	2	SoftConsult, a large Scandinavian supplier of IT-based solutions
74	(Ranganathan & Balaji, 2007)	Critical Capabilities for Offshore Outsourcing of Information Systems	MIS Quarterly Executive	IS Offshore Outsourcing Capabilities (Systemic Thinking, Vendor Management, Resource Management, and Change Management)	OM	2	Eighteen firms in IS offshore outsourcing
75	(El Sawy & Pavlou, 2008)	IT-Enabled Business Capabilities for Turbulent Environments	MIS Quarterly Executive	IT-enabled Business Capabilities (operational, dynamic, and improvisational)	TOM	2	Six Chief Information Systems Officer interviews

76	(Gorrieri et al., 2008)	Formal models and analysis of secure multicast in wired and wireless networks,	Journal of Automated Reasoning	Multicast communication and security issues	T	0	Gennaro and Rohatgi protocols
77	(Bauer et al., 2007)	Mobile Television: Challenges of Advanced Service Design	Communications of the Association for Information Systems	Mobile TV	OM	2	Mobile TV in South Korea
78	(Freed et al., 2007)	In-house development of scheduling decision support systems: Case study for scheduling semiconductor device test operations	International Journal of Production Research	In-House Systems Design	OM	2	Semicondutor Firm
79	(Vrontis et al., 2006)	Strategic marketing planning for a supplier of liquid food packaging products in Cyprus,	Journal of Business and Industrial Marketing	Strategic review of the marketing function	OM	2	Cypriot company operating in the liquid food packaging industry
80	(Goles et al., 2008)	Dark Screen: An Exercise in Cyber Security	MIS Quarterly Executive	Dark Screen (level of awareness, coordinating interorganizational responses, cyber incidents communications channels)	OM	0	Dark Screen exercise
81	(Petrovic-Lazarevic & Sohal, 2004)	Nature of e-business ethical dilemmas,	Information Management and Computer Security	CIO's ethical behavior	OM	2	Two Australian companies
82	(Magnuson et al., 2004)	Security aspects of electronic data interchange between a state health department and a hospital emergency department,	Journal of Public Health Management and Practice	Security Project	TOM	0	Hospital emergency department and a state public health department in Oregon
83	(Chien et al., 2003)	Entropia: Architecture and performance of an enterprise desktop grid system	Journal of Parallel and Distributed Computing	Computing Capacity (Physical Node Management, Resource Scheduling, and Job Management)	T	0	Entropia distributed computing system case
84	(R. Smith et al., 2021)	New Developments in Practice III: Riding the Wave: Extracting Value from Mobile Technology	Communications of the Association for Information Systems	Wireless technology	OM	2	A Santa Clara University study of ten firms currently using mobile computing in a variety of ways
85	(Verwoerd & Hunt, 2002)	Security architecture testing using IDS - A case study	Computer Communications	Security Verification Technique	T	0	Government Organization

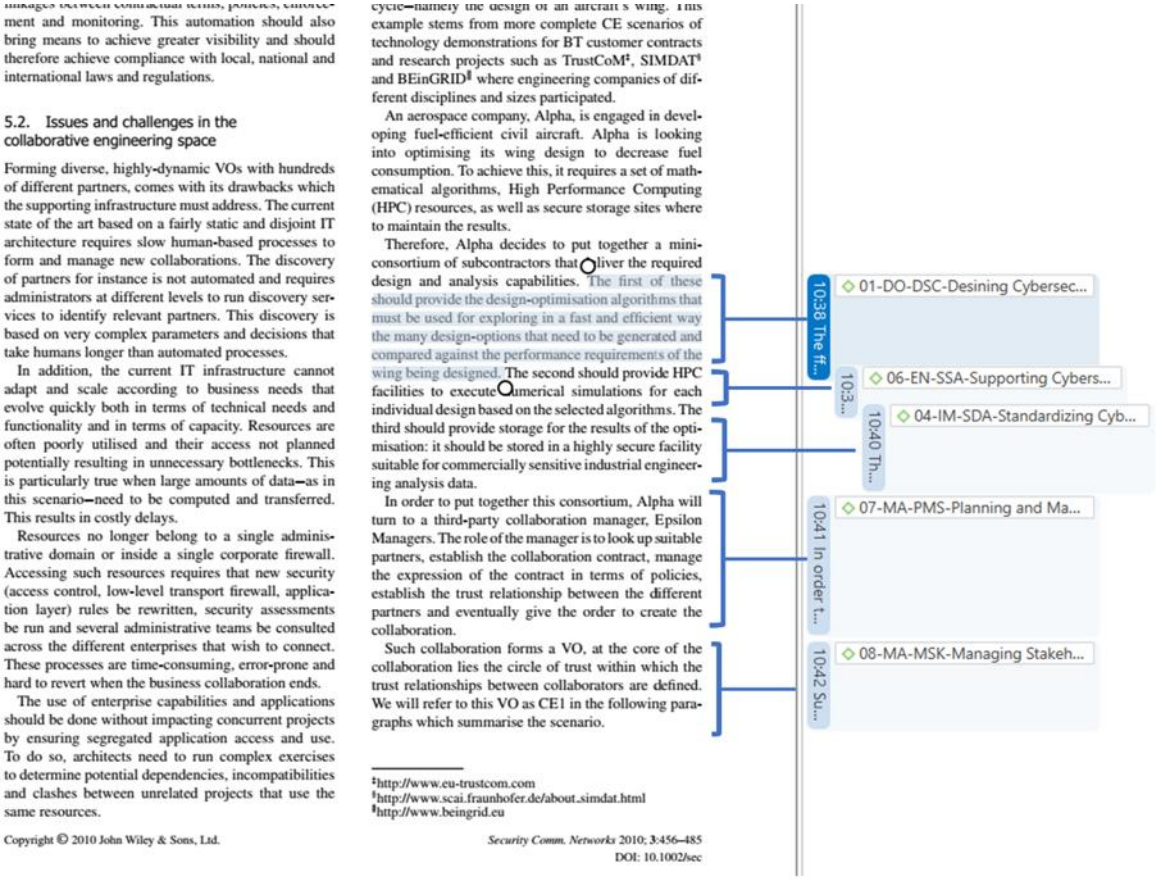
86	(Leizerov, 2000)	Privacy advocacy groups versus Intel: A case study of how social movements are tactically using the Internet to fight corporations,	Social Science Computer Review	Privacy Groups' Internet Protest Tactics	OM	2	Intel's controversial launch of the Pentium III® processor
87	(Dyerson & Mueller, 1999)	Learning, teamwork and appropriability: Managing technological change in the department of social security	Journal of Management Studies	Technological Capabilities Building	OM	2	Department of Social Security in UK
88	(Bailey et al., 1998)	Choosing successful technology development partners: A best-practice model	International Journal of Technology Management	Asset-light strategy	OM	2	Hotels in Markowitz's mixed assets portfolios
89	(Sayers, 1995)	Providing workplace literacy: Institutional collaboration with business and industry,	Community College Journal of Research and Practice	Basic skills programs	TOM	2	Texas Instruments Defense Systems Corporation and SGS-Thomson Microelectronics; Abbott Laboratories, J & E Die Casting, and Company X

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

2.8 APPENDIX C. CODING PROCESS

A coding structure approach in Atlas.ti provided in a case study evidence of DDCI framework (Figure C1). 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.

Figure C1. Coding Structure Approach in a case study using Atlas.ti Software



2.9 APPENDIX D. DYNAMIC CAPABILITIES IN CIBERSECURITY IDENTIFIED IN THE SAMPLE

#	Authors	DO-ESR	DO-DCS	DO-RDE	IM-DSA	EN-ISD	EN-SSA	MA-PMS	MA-MSK
1	(Abdul Molok et al., 2018)	0	3	0	0	0	3	2	3
2	(Ahmad et al., 2021)	0	1	1	12	5	2	14	5
3	(Aissani et al., 2012)	4	5	0	0	1	0	0	0
4	(Akinsanya et al., 2019)	2	1	0	1	0	0	1	0
5	(Al-Matari et al., 2021)	11	9	0	3	0	3	4	3
6	(Al-Matouq et al., 2020)	0	2	0	1	0	0	0	1
7	(Barletta et al., 2011)	0	5	0	0	0	0	0	0
8	(Bartnes & Moe, 2017)	2	0	0	1	5	2	0	1
9	(Blanco et al., 2015)	0	10	0	1	0	1	0	0
10	(Bradford et al., 2014)	2	2	2	5	3	2	4	0
11	(Brous & Janssen, 2020)	1	0	0	1	2	0	6	0
12	(Cahyani et al., 2017)	0	0	13	0	0	1	2	0
13	(Chatfield & Reddick, 2019)	0	1	0	2	4	1	2	1
14	(Chen et al., 2009)	0	2	0	3	0	0	3	0
15	(Chien et al., 2003)	0	0	0	0	0	0	0	0
16	(Corallo et al., 2012)	1	1	0	1	0	1	1	2
17	(de Leusse et al., 2010)	7	9	1	7	1	6	9	1
18	(Diaz et al., 2019)	8	6	0	1	0	8	1	0
19	(D'Orazio & Choo, 2018)	20	0	0	1	2	0	0	0
20	(Ghobakhloo & Fathi, 2019)	0	0	0	1	0	0	3	0
21	(Goles et al., 2008)	4	0	0	2	1	2	6	4
22	(Gong & Janssen, 2021)	6	3	0	4	3	6	4	0
23	(Goode & Lacey, 2021)	0	0	0	0	0	0	0	8
24	(Gorrieri et al., 2008)	0	14	0	0	0	0	0	0
25	(Humayun et al., 2022)	15	6	1	3	2	1	0	1
26	(Johansson et al., 2019)	0	2	0	1	0	0	0	0
27	(Kapoor et al., 2021)	0	0	0	1	0	2	0	1
28	(Laamanen & Wallin, 2009)	1	1	0	2	2	0	5	2

29	(Q. Li et al., 2019)	3	3	1	4	1	1	3	3
30	(Lu & Sinnott, 2018)	0	2	0	2	0	0	0	0
31	(Magnuson et al., 2004)	3	4	0	4	8	0	4	2
32	(Er et al., 2022)	1	4	0	4	1	0	2	3
33	(Mathrani & Lai, 2021)	9	8	0	11	0	3	1	0
34	(H. Naseer et al., 2021)	1	0	5	2	8	9	10	5
35	(A. Naseer et al., 2021)	2	1	0	0	0	4	1	0
36	(Attili et al., 2018)	5	2	0	2	6	0	4	16
37	(Rashidi & Rezakhani, 2017)	2	3	0	0	0	0	0	0
38	(Renwick & Gleasure, 2021)	2	5	0	1	2	2	1	3
39	(Seethamraju, 2015)	0	3	1	1	1	1	2	4
40	(R. Smith et al., 2021)	1	2	0	1	3	1	1	0
41	(Tan et al., 2016)	0	2	0	3	2	0	3	3
42	(Verwoerd & Hunt, 2002)	6	3	4	3	2	0	0	0
43	(W. Y. C. Wang et al., 2016)	0	0	3	0	0	0	0	0
44	(W. Wang et al., 2019)	1	11	0	4	9	1	6	2
45	(Williams et al., 2013)	2	0	0	3	3	3	9	2
46	(Yu et al., 2013)	1	2	2	0	0	2	0	0
47	(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.

3 STUDY 2. DYNAMICS CAPABILITIES IN CYBERSECURITY INTELLIGENCE: EMPIRICAL EVIDENCE TO ENHANCE PROTECTION AGAINST CYBER THREATS

This research addresses the relationship of dynamic capabilities in cybersecurity intelligence (DCCI) under the information security paradigm. Bolstering the view of cybersecurity intelligence (CI), the research looks at DCCI as a multidimensional critical framework of abilities and processes, particularly relevant for all business sectors somehow. The DCCI framework is built from a literature review of 47 case studies and tested from 207 cybersecurity experts spread out in different regions and countries through hierarchical regressions. The DDCI framework is positively associated with CI two different dimensions, Doing, and Improving cybersecurity activities while the dimensions Enabling and Managing cybersecurity activities do not present significant impacting in CI. To the best of the authors' knowledge, this is the first paper that build an empirical instrument to measure a model of dynamic capabilities in cybersecurity intelligence. Findings expand on the perception of CI as multidimensional problems involving firms' innovations and change in information security field. Thus, it progresses to offer new avenues for future research and practice in building DCCI to enhance CI for business and society.

3.1 INTRODUCTION AND CONTEXTUALIZATION

Fraud, malicious actions, cyber-attacks are a truly global problem affecting firms in different regions and industries worldwide. Measuring the true extent of the damage caused by these criminals disturbs to define what extent cybersecurity intelligence (CI) may protect a firm is challenger, due to the inherent nature of concealment involved in most schemes of cyber-criminal articulations. The Association of Certified Fraud Examiners (ACFE) estimates that firms' loss of revenue to fraud increase five percent each year after analyzing 2,110 cases in 133 countries representing a total losses of more than $3.6 billion (ACFE, 2022). Under this scenario, cybersecurity is a challenge evolving within technologies progress and high ambitious of cyber offenders (Malatji et al., 2022). Cybersecurity risks demands for firms high efforts in developing innovations, technical process, and abilities to attain preventative strategies as referred in literature of CI (Jasper, 2017; Kolini & Janczewski, 2022). Technological innovations as the most antecedent to build security features have also added further challenges for firms to create differentiation (Kosutic & Pigni, 2022).

However, excessive information security may negatively impact a firm's competitive advantage. In other words, it uncurtains others impacts such as on brand, crisis communication, business resumption, employees and public perception, customers retention, additional costs, third-party risks, firms' evaluation, among others. Thus, having a balanced approach requires a high level of capabilities to keep 'cybersecurity as a business enabler' [(Kosutic & Pigni, 2022) p.32]. Considering this scenario supported by a continuous improvement in the cybersecurity posture through capability models (Dube and Mohanty, 2020), the main motivation of this study is identifying how dynamic capabilities impact CI because many capabilities models have been subject to criticism because lack 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 arguments of some authors (Akinsanya et al., 2019; Dube & Mohanty, 2020) is to be always necessary to prescribe the to-be requirements to enhance cybersecurity posture and conduct an as-is analysis on a periodic interval to understand the updates in capabilities as an important perspective for theoretical and practical advancement.

Under this perspective, we posit the research question on *do dynamic capabilities in cybersecurity develop cybersecurity intelligence?* To answer this question, we present a framework of dynamic capabilities in cybersecurity (DCCI) as an approach tested empirically. The DCCI framework tested was built upon the Capability Maturity Model Integration (CMMI Institute, 2019) and the Building Security in Maturity Model (BSIMM, 2022), presenting four second order dynamic capabilities and eight first order dynamic capabilities. And as far as the authors know, this is the first time that these models are combined into one and tested empirically. Conceptualizing dynamic capabilities in cybersecurity as of processes and abilities to identify, mobilize and renewal resources against cyber fraud, this study also highlights CI, following Kolini and Janczewski (2022), and defining CI 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). Therefore, the number of innovations, organizational changes and performance throughout cybersecurity are relevant measures to CI analysis.

Additionally, the theories of Diamond Fraud and Dynamic Capabilities sustain the theoretical basis of this study because some reasons: first, Diamond Fraud Theory has a central perspective of capabilities to recognize opportunities to walk through fraudulent actions under a camouflage, and the central challenge of CI is mitigating these actions. Second, Dynamic Capabilities theory offers structured microfoundations about processes and abilities in relevant

fit in dynamic environments as found in cybersecurity scenario. And third, both Diamond Fraud theory and Dynamic Capabilities theory are useful on the individual and organizational level. As result, findings reveal that CI is positively associated with Doing and Improving cybersecurity activities while Enabling and Managing cybersecurity activities do not present significant impact, empirically.

This study contributes to the current literature in three ways: (1) it tests empirically a new framework of DDCI to raise new perspectives for the development of cybersecurity capabilities, while accounting the impact of innovations, organizational cybersecurity change and performance; (2) it offers new measures for cybersecurity capabilities and cybersecurity intelligence; (3) it strengthens how capabilities are deeply associated in CI reinforming the value of Dynamic Capabilities and Diamond Fraud theories for cybersecurity research field; and (4) it brings the current status of perception from the experts about capabilities in cybersecurity intelligence.

This research is also based on two operating assumptions, as follows: (1) the increasing number of cybercriminal articulations have aggravated the firms cyber-risk climate demanding CI enhancements, and (2) there is a need for a better understanding of what are and how the DCCI respond to the potential of CI development against cyberattacks. The assumptions are presented in section 2, given their relevance to the hypotheses upon which this research is founded. In section 3, it describes the methodological approach, with a focus on how data were collected from cybersecurity experts through hierarchical regressions. And the results are presented and discussed in sections 4 and 5 respectively, followed by the conclusions of the study in section 6.

3.2 THEORETICAL MODEL AND HYPOTHESIS DEVELOPMENT

This research model investigates the influence of dynamic capabilities in cybersecurity (DCCI) on cybersecurity intelligence (CI). Our research model brings together fraud diamond and dynamic capabilities theories to identify the capabilities of cybersecurity innovations (new technologies and processes implemented), organizational change (controls proactively implemented before a cyberattack happens), and performance (new security threat actors identified highlighting gaps in the firm's cyber defenses). We conceptualize the DCCI framework under the structure of the Capability Maturity Model Integration (CMMI Institute, 2019), which consists of four main categories: DOING for developing quality products, ENABLING for supporting the development of products, IMPROVING for cybersecurity

performance, and MANAGING for planning cybersecurity activities and handling stakeholders (Al-Matouq et al., 2020; CMMI Institute, 2019). All four dimensions, combined with various activities presented by the Building Security in Maturity Model (BSIMM, 2022), theorize about CI and dynamic capabilities to demonstrate a new perspective.

3.2.1 Theoretical Positioning: Fraud Diamond and Dynamic Capabilities Theories

Fraud diamond theory indicates that fraud will not occur if the perpetrator cannot recognize opportunities to engage in fraudulent actions under camouflage (Wolfe & Hermanson, 2004). Audit bodies and practitioners recognized the theory as a theoretical model to explain the occurrence of cybersecurity incidents. It acts as an "early fraud warning instrument" in fraud cases, according to Rustiarini et al. (2022) and Gill (2011). The term capability is seen as differentiating skills that each cyber offender possesses (Cieslewicz, 2012; Gill, 2011; Rustiarini et al., 2019).

Furthermore, fraud diamond theory considers four directions of fraud (pressure, opportunity, rationalization, and capability), stating capability closer to the perpetrator in "strategic position" as well as "adequate knowledge". This suggests that major fraud comes from deliberate, imaginative, knowledgeable, and bright people with a strong awareness of firms' controls (ACFE, 2022; Ramamoorti et al., 2009; Saluja et al., 2021). According to the Association Certified Fraud Examiners Report (2022), eighty-one percent of firms that are victims of fraud modified their anti-fraud controls after the fraud, with seventy-five percent increasing management review procedures and sixty-four percent enhancing the use of proactive data monitoring and analysis (ACFE, 2022).

According to Saluja et al. (2021), "fraud is a cultured and active process that adjusts to the present environment on a regular basis" (p. 1326), corroborating the statement of Steinmetz (2015), who mentioned that "it is not enough to approach things in a logical and critical capacity, but one has to be willing to think unorthodoxly to fight against fraud" (p. 131). Other authors (Mansor, 2015; Saluja et al., 2021) also highlighted that capability represents the potential perpetrator to commit fraud. Albrecht, Albrecht, and Albrecht (2008), cited in Saluja et al. (2021), believed that "the individuals who have extremely high capability will understand the ongoing internal control system and would recognize the weaknesses in the organization to use this capability and skills in planning something fraudulent" [(Albrecht et al., 2008; Saluja et al., 2021), p. 1322].

Under the theory of dynamic capabilities already structured in its microfoundations, the question about capability indicated in diamond fraud as being personal traits and abilities to determine whether fraud will occur in the presence of pressure, opportunity, and rationalization gives the chance to highlight the capabilities from defenders against offenders as part of an organized framework that may represent an organizational shield against digital fraud (Vousinas, 2019).

Dynamic capabilities theory may support and explain how firms reframe their value generation through information technologies (Schryen, 2015; Steininger et al., 2022). Doing so may complement information technologies business value by highlighting abilities (i.e., the usability of historical data on a real-time basis to separately determine how best to plan and manage cybersecurity in the future) or processes (i.e., introducing proper activities to revise security designs) enabled by technologies designed for cyber defense (Steininger et al., 2022).

Considering information technology (IT) as a tool for substituting labor or improving productivity, data processing, or social relations (Orlikowski & Iacono, 2001; Steininger et al., 2022), the three microfoundations of capacities, regarding abilities and processes, that form the structure of dynamic capabilities (Teece, 2007, 2012) might be conceptualized from the IT perspective as (1) *sensing* to identify and assess cyber opportunities and threats, (2) *seizing* to mobilize resources to address such opportunities or threats to capture value from doing so, and (3) *transforming* to continue renewal. Hence, firms that engage in continuous or semicontinuous sensing, seizing, and transforming have more chances to sustain themselves in the face of cyberattacks (Steininger et al., 2022).

Beyond all conceptual and theoretical considerations about dynamic capabilities in IT, Steininger et al. (2022) highlight that a growing body of empirical research explores the use of dynamic capabilities theory to explain IT-related phenomena. Dynamic capabilities may be the outcome or a mediator toward technological performance (Karimi & Walter, 2015), yet IT-embedded dynamic capabilities are also theorized as being antecedents for organizational change or performance outcomes (Mikalef et al., 2021; Vial, 2019; Wang et al., 2015). They expand organizational boundaries by incorporating critical resources (Y.-H. Li & Huang, 2013) and can accelerate the speed at which firms react (Queiroz et al., 2018; Steininger et al., 2022; Wei & Wang, 2010). Thus, under this theoretical perspective, we conceptualize dynamic capabilities in cybersecurity as processes and abilities to identify, mobilize, and renew resources against fraud in the cyber environment to potentialize firms' cybersecurity intelligence.

3.2.2 Dynamic Capabilities in Cybersecurity (DCCI)

To conceptualize dynamic capabilities in cybersecurity (DCCI), a framework must be outlined from the cybersecurity capabilities perspective of the heterogeneous body of literature in this research field. Based on our research model, we included core capabilities and best practices in cybersecurity as maturity-dependent components adapted from the Capability Maturity Model Integration (CMMI Institute, 2019) that enables firms to build, assess, and improve their processes and abilities. To describe the essential structure of our DCCI framework, we used the Building Security in Maturity Model (BSIMM, 2022). TA team of leading software security experts developed the BSIMM in 2008 by quantifying the security practices of many firms through a total of one hundred nineteen activities in information security. It represents the various needs, objectives, and expectations of firms according to their domain of technical complexity of doing, enabling, supporting, planning, and managing cybersecurity. According to Garcia-Perez et al. (2021), this is particularly important given the broad scope of cybersecurity through its general focus on the critical technical environment in firms (Garcia-Perez et al., 2021).

A comprehensive approach in which dynamic capabilities ensure outcomes, changes, and adequate technological performance, despite potential incidents or failures in information systems, is evidenced among researchers (Karimi & Walter, 2021; H. Naseer et al., 2021; Steininger et al., 2022; W. Wang et al., 2019). Cybersecurity capabilities primarily aim only at technical skills and knowledge to avoid these incidents and failures (Ani et al., 2019; Carlton et al., 2019; Srivatanakul & Annansingh, 2021). Therefore, our DCCI framework combined both perspectives to describe dynamic capabilities as processes and abilities to develop CI.

Our DCCI framework also analyzed the microfoundations of dynamic capabilities: sensing, seizing, and transforming (Teece, 2007, 2012) to organize the Capability Maturity Model Integration (CMMI) and the Building Security in Maturity Model (BSIMM, 2022). This process proposes four dimensions (1) Doing dynamic capabilities to develop quality cybersecurity products; (2) Enabling for supporting the development of products; (3) Improving cybersecurity performance, and (4) Managing for planning cybersecurity activities and handling stakeholders (Al-Matouq et al., 2020; BSIMM, 2022; CMMI Institute, 2019).

The framework is theoretically structured upon first-order capabilities related to the organizational cybersecurity activities found in the Building Security in Maturity Model literature (BSIMM, 2022), which organizes the ways of operating cybersecurity. The second-order capabilities from Capability Maturity Model Integration (CMMI) reflect organizational

outcomes. Both structures were analyzed and compared with the structures of the construct dynamic capabilities microfoundations (sensing, seizing, and transforming). Table 5 presents the dimensions of dynamic capabilities and their microfoundations.

Table 5. DDCI Consolidated Framework

2nd order	1st order	Micro foundations	Outcomes	References
Doing Cybersecurity	Engineering Cybersecurity Requirements	Sensing	Processes Intensifying Organizational Change	(Attili et al., 2018; Bartnes & Moe, 2017; Diaz et al., 2019; Goles et al., 2008; Goode & Lacey, 2021; Mathrani & Lai, 2021)
	Design Cybersecurity Solutions	Sensing	Processes Intensifying Organizational Change	(Goode & Lacey, 2021; Magnuson et al., 2004; Seethamraju, 2015; W. Wang et al., 2019)
	Review Cybersecurity Design	Sensing	Processes Intensifying Organizational Change	(Cahyani et al., 2017; Goode & Lacey, 2021; H. Naseer et al., 2021; W. Y. C. Wang et al., 2016)
Improving Cybersecurity	Standardize Cybersecurity Activities	Seizing	Processes Intensifying Organizational Change	(Abdul Molok et al., 2018; Ahmad et al., 2021; Bradford et al., 2014; Seethamraju, 2015; Williams et al., 2013)
	Improve Cybersecurity	Sensing/ Transforming	Processes and Abilities Intensifying Organizational Change and Performance	(Abdul Molok et al., 2018; Al-Matouq et al., 2020; Goode & Lacey, 2021; Magnuson et al., 2004; H. Naseer et al., 2021; Tan et al., 2016; W. Wang et al., 2019)
Enabling Cybersecurity	Support Cybersecurity Activities	Transforming	Processes and Abilities Intensifying Organizational Change	(Abdul Molok et al., 2018; Ahmad et al., 2021; Bartnes & Moe, 2017; Cahyani et al., 2017; Diaz et al., 2019; Goles et al., 2008; Goode & Lacey, 2021; A. Naseer et al., 2021; Tan et al., 2016; Williams et al., 2013)
Managing Cybersecurity	Plan & Manage Cybersecurity	Seizing	Processes and Abilities Intensifying Organizational Change	(Ahmad et al., 2021; Akinsanya et al., 2019; Goode & Lacey, 2021; Laamanen & Wallin, 2009; Magnuson et al., 2004; H. Naseer et al., 2021; Renwick & Gleasure, 2021; Tan et al., 2016; W. Wang et al., 2019; Williams et al., 2013)
	Manage Stakeholders	Seizing	Abilities Intensifying Organizational Change and Performance	(Abdul Molok et al., 2018; Ahmad et al., 2021; Attili et al., 2018; Bartnes & Moe, 2017; H. Naseer et al., 2021; Tan et al., 2016; W. Wang et al., 2019)

Source: Framework built as of the Building Security in Maturity Model literature (BSIMM, 2022), Capability Maturity Model Integration (CMMI), Dynamic Capabilities Microfoundations (Steininger et al., 2022; Teece, 2018) and DCCI framework (Pigola & da Costa, 2023).

As various cybersecurity tools, processes, techniques, and procedures have been developed over the years (Dellios et al., 2015; Malatji et al., 2022), the evolution of firms' cybersecurity capabilities (skills and knowledge) has increased. However, building capabilities

in cybersecurity is extremely involved with a variety of economic and organizational parameters (Garcia-Perez et al., 2021). It may vary largely based on firms' size, technological dependence, area of operation, business model, country context, asset availability, and other stakeholders' risks. Thus, it may affect the nature and scope of meaningful responses for the constructs.

To address the variability of cybersecurity capabilities, we followed Garcia-Perez et al. (2021) by applying common constructs that are not intrinsically susceptible to idiosyncrasies, such as only senior professionals' perceptions. Specifically, considering the dynamism in the cybersecurity field, we also follow the drivers highlighted by Pigola and da Costa (2023), in our DCCI framework as a common sense of capabilities by joining theoretical and empirical perspectives (Pigola & da Costa, 2023).

Additionally, we identified the most relevant aspects in these scenarios as organizational change and performance in cybersecurity (i.e., new-threats actors' identification, security controls, secure data analytics sources, and innovative technologies and technical processes for cyber defense). Even though it does not completely embrace the challenges in terms of capabilities development, the component of responses permits tracking various indicators in Doing, Enabling, Improving, and Managing cybersecurity across different firms through logic imputes and common responses. This allows for a richer interpretation of findings considering that different scenarios and patterns may be derived. Table 4 displays and further elaborates on the definitions of each DCCI.

3.2.3 Cybersecurity Intelligence

Cybersecurity intelligence (CI) appears in literature under various perspectives, such as big data analytics (Al Jallad et al., 2020; Rao et al., 2016), malware, misuse, or stealthy communication (Aharoni et al., 2016; Schales et al., 2016), internet of things (Mishra et al., 2022; Stoecklin et al., 2016), cloud security (Amrein et al., 2016; Berger et al., 2016), insider threats (Coden et al., 2016), misuse of authorizations (Chari et al., 2016), and privacy vulnerabilities (Gkoulalas-Divanis & Braghin, 2016).

Recently, Kolini and Janczewski (2022) introduced a framework for CI to develop broader information security awareness to respond quickly to large-scale cyberattacks to protect critical assets. The framework is multidimensional and contemplates technological, environmental, and inter/intraorganizational factors. In other words, the authors mentioned that 'CI 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]. CI also helps firms prioritize their defense capabilities to safeguard the most vulnerable assets (Jasper, 2017). Furthermore, the term CI appears interchangeably, such as 'cloud security intelligence' (Berger et al., 2016), 'threat intelligence' (Hu et al., 2016), or 'big data security intelligence' [(starting in 2007);(Rao, 2016)].

Cybersecurity intelligence gathers organizational and technical demands for asset protection to give firms the capacity to predict vulnerabilities and identify threat actors (Kolini & Janczewski, 2022). However, cybersecurity operations are complex, and they may postpone expected outcomes. Such complexities are mostly related to the absence of capabilities in designing cybersecurity infrastructure, identifying data-quality issues, developing automation, and managing stakeholders, among other challenges (Carlton et al., 2019; Jalali et al., 2019; Kolini & Janczewski, 2022; Tounsi & Rais, 2018). However, reliable CI in a fast time frame is only possible in the presence of interoperability of security platforms and quality security networks created by a high maturity level of cybersecurity capabilities (CMMI Institute, 2019; Doyle, 2018; Kolini & Janczewski, 2022). Table 6 summarizes some perspectives of CI found in literature.

Table 6. Authors' perspectives on Cybersecurity Intelligence

Definitions	References
Security networks and security-related information, such as risks, vulnerabilities, incidents, and remediation activities.	(N. Robinson & Disley, 2010)
The process of acquiring and analyzing information to identify, track, and predict cyberattacks.	(Jasper, 2017; Mutemwa et al., 2017; Townsend et al., 2013)
Low-level compromise indicators (e.g., malware hash-value, malicious IP addresses) that require immediate action through an automated response.	(Brown et al., 2015)
Contextual data from logical and analytical processes, which a human agent often evaluates for accuracy and quality.	(Dalziel et al., 2015; Tounsi & Rais, 2018)
Includes context, evidence-based knowledge, mechanisms, indicators, actionable advice, and implications about emerging or existing threats used to inform decisions regarding the subject's response to that menace or hazard.	(Qiang et al., 2017)
Refers to structured, relevant, dependable, and timely information that one can action to improve security posture.	(Mtsweni et al., 2016)
Provides knowledge of an attacker's capabilities, motives, resources, and objectives to assist firms in their decision-making processes and enhance their defense strategies.	(Kolini & Janczewski, 2022)

Source. Elaborated by the Author (2022)

The approach provided by Kolini and Jaczewski (2022) highlighted the need to explore CI under multidisciplinary paradigms to ensure CI determinants in practice for information security improvement, which involves not only technology but also organizational process

changes, innovations, and performance. The authors mentioned that “the factors including information quality, information confidentiality, intelligence-sharing standards, technology complexity (technology factors), organizational cost, organizational performance, information confidentiality, organizational readiness (intraorganizational factors), trust relationships, reciprocity, information assurance (interorganizational factors), law and regulations, competition in the market, and external pressure (environmental factors) are associated in the CI framework”. [(Kolini & Janczewski, 2022) p. 50].

Considering the heterogenous dimensions that CI assumed in literature and the perspective of information security technology development, we defined CI 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. Therefore, the number of innovations, organizational changes and performance throughout cybersecurity are relevant to measures CI. Innovations because the number of new information security technologies and processes developed, implemented, or experimented with are relevant to monitor and detect cyber-threats. Organizational factors change are security controls proactively implemented and increase of data sources in the network because they promote appropriate visibility about trustable resources into network transactions to enhance the defenses. And environmental factors like threat-actors identification to performance in CI is the main objective to mitigate cyber threats.

3.3 HYPOTHESES DEVELOPMENT

Having identified the four components of the DCCI framework that potentially may influence CI, one important premise for our first hypothesis is that CI supports critical asset protection and predicts cyber threats before a fraud cyber offender acts (Kolini & Janczewski, 2022). The number of cybersecurity sources, stakeholder limitations, and intelligence-enrichment difficulties cause struggles for firms in managing their CI (Abdul Molok et al., 2018; Ahmad et al., 2021; Attili et al., 2018; Bartnes & Moe, 2017; Goode & Lacey, 2021; H. Naseer et al., 2021; Seethamraju, 2015; Tan et al., 2016; W. Wang et al., 2019). In this vein, firms must increase their stakeholders’ alignment about cybersecurity to minimize the likelihood of cyberattacks (Jalali & Kaiser, 2018).

Firms also pay attention to training users to raise awareness about the criticalities in cybersecurity defense to avoid the incorrect dissemination of data (Abdul Molok et al., 2018; Seethamraju, 2015). However, firms invest time to persuade users to accept the integrated

nature of the systems (Seethamraju, 2015). Firms may also manage security data generated by the different providers that offer different systems from various sources in the form of logs such as firewalls, intrusion detection and prevention systems, applications, databases, and servers (A. Naseer et al., 2021). Moreover, any implementation of laws and regulations may control market-oriented behaviors impacting the evolution of CI in firms (Q. Li et al., 2019).

These interrelations among different areas and issues related to cybersecurity to create a cyber defense demand a firm's strong attention in managing their level of cybersecurity capabilities to shift CI accordingly without impacting business operations. Therefore, we hypothesize that *firms that potentialize managing activities in cybersecurity are more likely to be oriented toward cybersecurity intelligence* (H1).

According to Jalali et al. (2018), 'cybersecurity capabilities include a variety of programs, behaviors, and technologies employed to improve cyber resiliency'. However, not all capabilities are self-sustaining, and even when properly adopted, the dynamism of the cybersecurity field demands improvements to impact firms' ability to be resilient to new cyberattacks (Jalali et al., 2019). Vogel (2016) also highlights that reskilling and upskilling in cyber expertise is essential in dealing with dynamic and technically savvy cyber opponents. This means that firms need to invest in technical capabilities to improve their cybersecurity capacity (Vogel, 2016).

Practitioners should know the status of information security to make decisions about the appropriate technological infrastructure and security design to address their cybersecurity needs. This means that they need a set of technical skills to create new skills to improve their intelligence in cybersecurity (Diesch et al., 2018, 2020; Horne et al., 2017). Embeddedness in the DCCI enhances the appropriateness of technical choices to build CI (Elragal & Haddara, 2012; Marinho et al., 2021); therefore, we hypothesize that *there is a positive effect between doing cybersecurity and cybersecurity intelligence* (H2).

Innovative resistant security measures and improvements in security processes and abilities in the next generation of cyber experts will remain a critical initiative for CI effectiveness (Ahmad et al., 2021; Elmo et al., 2020; Ikeda et al., 2019). Nasser et al. (2021) mentioned that the standardization of information from different information security sources with threat intelligence feeds the analysis of monitoring dashboards that help firms improve the cybersecurity awareness of their managers. This awareness through supportive security technologies and associated activities particularly impacted CI related to the cyberattacks attempted on firms' networks (H. Naseer et al., 2021). Our efforts to understand the association between supportive activities in cybersecurity enabling information security changes to

provoke firms' CI enhancements led us to hypothesize *firms that simultaneously emphasize enabling cybersecurity activities support cybersecurity intelligence* (H3).

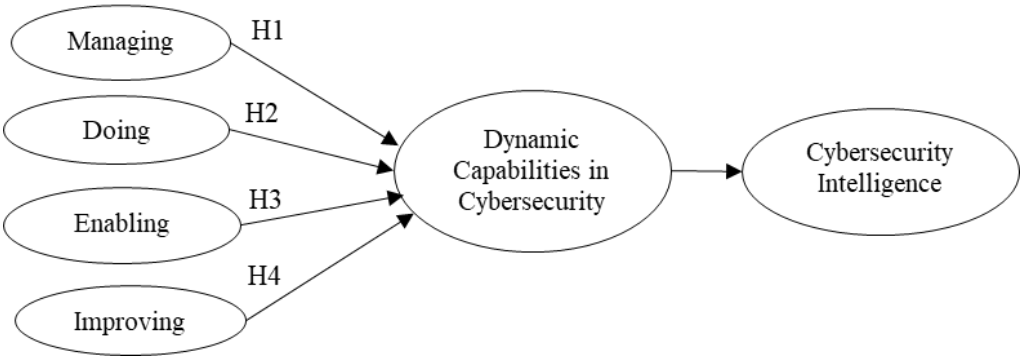
Improving cybersecurity activities involves different dynamic capability microfoundations (sensing, seizing, and transforming). This perspective reintroduces the CI viewpoint provided by Kolini and Janczewski (2022), who highlight that the visibility of an attacker's capabilities, motives, resources, and objectives assists firms in decision-making processes and enhancements in defense strategies. This visibility requires being willing to think unorthodoxly, as emphasized by Steinmetz (2015), to demand immediate action. Consequently, cyber defenders must constantly improve cybersecurity activities to attend to new cyber challenges. However, relevant, standardized, timely, and reliable data sources may improve security posture to sustain firms' CI preparedness (Kolini & Janczewski, 2022; Mtsweni et al., 2016).

Tounsi and Rais (2018) suggested a standardized security vocabulary for threat intelligence feeds to assist firms in customizing their CI sharing tools and search capabilities required for daily tasks (Kolini & Janczewski, 2022; Serrano et al., 2014; Tounsi & Rais, 2018). Other authors (Brown et al., 2015) have noted that technology standardization defines normalized data models for detecting and responding to security events. However, according to Kolini and Janczewski (2022), these models are not sufficient to increase interoperability between CI platforms. To improve the quality of CI networks and provide a more reliable CI in a faster time frame, there is a need to consistently improve other cybersecurity activities. Therefore, we hypothesize that *there is a positive effect between improving cybersecurity and cybersecurity intelligence* (H4).

Given the theoretical bases of the study, we argue that once firms build DCCIs, they may positively influence CI.

Figure 3 depicts our conceptual research model.

Figure 3. Conceptual Model



Source: Elaborated by author (2022)

3.4 RESEARCH METHOD

3.4.1 Data

The research model conducts a survey to collect data from information security experts in different countries to validate our DCCI framework. Over six months (between Feb 2022 and Aug 2022), we distributed an online survey via e-mail among experts in cybersecurity in various business sectors. They were asked to give information about their business environment and not their personal opinion about cybersecurity capabilities. Preceding the survey, two specialists with more than 20 years in cybersecurity working in different industries, one in finance industry and the other in technology industry, validated the questionnaire. In a sequence, we pre-tested a preliminary version of the questionnaire through forty respondents, resulting in some adjustments in the semantics of questions. We sent personalized e-mails in English with a unique link to the survey to a total of 1,729 e-mail addresses drawn from LinkedIn (a database containing information on firms' professionals). In total, we received 350 responses, of which 207 were completed and 143 were noncompleted. This gives us an effective response rate of 11.97%.

The experts in our sample cover a wide range of industries and countries (See Table 7). For instance, the financial sector is the majority industry, and the technology industry covers five categories: data protection, electrical and electronic, graphic technology, information management, and internet of things. To avoid potential problems related to common-method variance at the start of the survey, we assured the anonymity of participants and the confidentiality of the study, that there are no right or wrong answers and that they should answer the questions as honestly as possible.

The relationships between the independent and dependent variables are novel and complex, including several formative effects; therefore, we used the QuestionPro survey platform to prevent participants from being guided by a cognitive map that included difficult-to-visualize interactions. The items related to the constructs include several reverse-coded items, which reduced the likelihood of participants giving similar answers to the items. To ensure the quality of the information obtained, we asked respondents about their experience and job position to ensure that they could offer quality information (See Table 8). The sample includes experts from all categories. Therefore, we reasonably assume that the respondents have in-depth knowledge about capabilities in cybersecurity.

Table 7. Overview countries and industries responses

Industry Sector	Total	Percentage	Location	Total	Percentage
Aerospace and Aviation	3	1.46	Argentina	4	1.95
Agriculture	1	0.49	Australia	13	6.34
Automotive	6	2.91	Brazil	35	17.07
Construction and Building	4	1.94	Canada	16	7.80
CSR and governance	1	0.49	Denmark	1	0.49
Customer service	5	2.43	France	2	0.98
Data protection	15	7.28	Germany	17	8.29
Education	3	1.46	India	19	9.27
Electrical and electronic	2	0.97	Israel	3	1.46
Energy and utilities	4	1.94	Italy	13	6.34
Engineering	4	1.94	Japan	3	1.46
Environmental & Sustainability	1	0.49	Mexico	23	11.17
Financial services	53	25.24	New Zealand	1	0.49
Food and drink	3	1.46	Nigeria	1	0.49
Government	1	0.49	Portugal	6	2.93
Graphic technology	1	0.49	Qatar	1	0.49
Health and Safety	10	4.83	Rwanda	1	0.49
ICT and Telecoms	20	9.66	South Africa	13	6.34
Import export	2	0.97	Spain	6	2.93
Information management	12	5.83	Sweden	1	0.49
Innovation and design	1	0.49	Switzerland	12	5.85
Internet of Things	2	0.97	United States	16	7.80
Logistics and Transportation	5	1.46			
Manufacturing and processing	10	4.85			
Medical devices	2	0.97			
Mining	1	0.49			
Other	14	6.80			
Retail	4	1.94			
Services	17	8.21			

Note. Elaborated by Author (2022)
Legend. CSR = Corporate and Social Responsibility; ICT = Information and communications technology; IT = Information Technology

Table 8. Overview of job position and cybersecurity experience responses

Job Position	Total	Percentage	Experience in Cybersecurity	Total	Percentage
Chief Officer	46	22.55	Less than 3 years	14	6.83
Director	12	5.88	4 to 7 years	48	23.18

Manager	60	29.41	8 to 10 years	30	14.63
Expert	68	32.85	10 to 13 years	28	13.66
Other	21	10.19	Above 14	87	42.23

Source. Elaborated by Author (2022)

3.4.2 Measures

3.4.2.1 Dependent Variables

Cybersecurity intelligence is measured through five indicators. We asked experts whether their firm has developed innovations, cybersecurity changes, and performance on a five-point Likert scale (from 1 = ‘strongly disagree’ to 5 = ‘strongly agree’). We consider CI as the new information security technologies implemented (NIC1), new information security processes developed (NIC2), implemented or experimented with, new security controls (OCC1), the number of information security data sources in the network (OCC2), and the number of identified new security threat actors highlighting gaps in cyber defenses (OCP) (Ahmad et al., 2021; Dani & Gandhi, 2021; Elmo et al., 2020; Naseer et al., 2021; Sprong et al., 2021).

3.4.2.2 Independent Variables

Doing, improving, enabling, and managing cybersecurity are constructs of the second order built from the eight constructs of the first order. Doing is measured by engineering cybersecurity requirements (ECR), designing cybersecurity solutions (DSR), and reviewing cybersecurity design (RCD). Improving is measured by standardizing cybersecurity activities (SCA) and improving cybersecurity (IMC). Enabling is measured by supporting cybersecurity activities (SPA). Managing is measured by planning and managing cybersecurity (PMC) and managing stakeholders (MAS) (Al-Matouq et al., 2020; BSIMM, 2022; CMMI Institute, 2019). The survey asked respondents to rate each statement using a five-point Likert scale (from 1 = ‘strongly disagree’ to 5 = ‘strongly agree’). Appendix E presents the entire instrument applied in the survey.

3.4.2.3 Variables of Controls

The two control variables are job position and experience in cybersecurity. The job position is an ordinal variable consisting of five separate ranges of categories (5 = Chief Officer; 4 = Director; 3 = Manager; 2 = Expert; and 1 = Other). Experience is also an ordinal variable consisting of five separate ranges of categories (1 = less than 3 years; 2 = 4 to 7 years; 3 = 8 to 10 years; 4 = 10 to 13 years; and 5 = above 14). We track these variables to understand their level of influence considering that a potential variability of knowledge in each job position may exist and that the impact of experience on capabilities may be varied to influence cybersecurity posture to build CI.

3.4.3 Data Analysis

We performed an exploratory factor analysis (EFA) with FACTOR 10 software (Ferrando & Lorenzo-Seva, 2017; Gibson Jr. et al., 2020), using parallel analysis as the extraction method to measure each factor. As recommended by some authors (Harerimana & Mtshali, 2020; Wollack et al., 2003), the first step involved the overall reliability, which at 0.942 was above the minimum acceptable of 0.70. In the initial factor analysis (EFA) phase, we screened data using the Kaiser–Meyer–Olkin (KMO) measure of sampling adequacy (0.938), which was acceptable at >0.50, and Bartlett's test of sphericity (2,223.9 (741) p <.001), which was acceptable at $p < 0.05$. For factor loading retention, the higher the variable loadings, the stronger the factor solution of a particular common factor. We found recommendations in literature to use thresholds above 0.32 (Gibson Jr. et al., 2020; Tabachnick & Fidell, 2014) and above 0.50 (Sharma et al., 2005).

However, we decided to use the recommendations of Howard (2016) and the.40–.30–.20 rule This rule consists of a satisfactory variable that should (1) load onto their primary factor above 0.40, (2) load onto alternative factors below 0.30, and (3) demonstrate a difference of 0.20 between their primary and alternative factor loadings to validate our instrument (Harerimana & Mtshali, 2020; Howard, 2016). The coefficients for items are displayed by factors, with all factor numbers above 0.40, and the extracted factors are explained by a total variance of 48.02% (overall Cronbach's α >.938, AVE >.736, CR >.723). Appendix E provides the factor loadings of the entire instrument and measures of each indicator of the variables.

To validate our constructs' replicability, we use the generalized H index (Ferrando & Lorenzo-Seva, 2018; Pigola & Da Costa, 2021). The H index evaluates how well a set of items represents a common factor. It is bounded between 0 and 1 and approaches unity as the magnitude of the factor loadings and/or the number of items increases. Higher H values (=>0.80) suggest a well-defined and stable latent variable. Our latent variables were 0.966 for DCCI and 0.905 for CI. For the quality and effectiveness of factor score estimates, Ferrando & Lorenzo-Seva (2018) recommend applying an expected percentage of true differences (EPTD) above 90%, which is the estimated percentage of differences between the observed factor score estimates that are in the same direction as the corresponding true differences, marginal reliabilities above 0.80, factor determinacy index (FDI) values above 0.90, and sensitivity ratio (S_R) above 2, which can be interpreted as the number of different factor levels than can be differentiated based on the factor score estimates (Ferrando and Lorenzo-Seva, 2018). Table 9 presents the indexes of quality and effectiveness of factor score estimates.

Table 9. Quality and effectiveness of factor scores estimates.

	DCCI	CI
FDI - factor determinacy index	.983	.951
Marginal Reliability	.966	.905
S_R - sensitivity ratio	5.364	3.092
EPTD - expected percentage of true differences	96.6%	92.7%

Source: (Ferrando & Lorenzo-Seva, 2018)

Next, to determine the second order and first order of the measures, we created composite variables that take the measures mean for each construct. We ran separate linear regressions in JASP software to test the effect on the dependent variable. Third, we analyzed the endogeneity of the variables using r software, applying Hausman's specification test (if the OLS and IV regression produce significantly different estimates, then the suspected independent variables are endogenous), weak instrument test (Cragg Donald-F statistic should be < 10), and Sargan-Hansen Test (p-value must not be less < 5% and > 10%). We also utilized the Wald test with a p-value less than the generally used criterion of 0.05, so we can reject the null hypothesis, indicating that the coefficients are not simultaneously equal to zero. Including statistically significant predictors should lead to better predictions (i.e., better model fit); we can conclude that the analyzed factors result in a statistically significant improvement in the fit of the model. Table 10 presents the endogeneity results. (Daryanto, 2020; Hausman, 1978; Y. Lee & Okui, 2012; Stock & Watson, 2019). Finally, we compared the F-statistics and differences in R^2 of the regression models.

Table 10. Endogeneity Tests

Diagnostic	DOING	IMPROVING	ENABLING	MANAGING
Wu-Hausman	1.148(.285)	3.457(.065)	26.409(.125)	11.199 (.101)
Weak instruments	169.153(***)	148.547(***)	143.504(***)	180.535 (***)
Sargan-Hansen	4.634 (.099)	7.754 (.051)	4.893(.087)	9.046(.060)
Estimates	0.927 [.139]	0.761[0.116]	0.7516 [.116]	0.711[.108]
Wald test	44.31 (***)	43.14 (***)	41.98 (***)	43.59(***)

Note. pvalue in parentheses. *** = p < 0.001. Standard Error in brackets

We analyze the data through hierarchical linear regressions in JASP by conducting a series of regression analyses, each time adding the two control variables with the explanatory variables into each model. Obtaining generalizability of the results requires a ratio of observations to independent variables of at least five to one and preferably fifteen to one (Hair et al., 2009). We work with ten variables (i.e., two control variables and eight independent variables to analyze the first-order constructs and four independent variables plus two control variables to analyze the second-order constructs). In our sample, 207 cases provide valid

information, which is within the suggested number of cases to run the analyses (Howard, 2016). Table 11 shows the descriptive statistics and the bivariate correlations among the variables. The highest correlations are between Doing and Managing (r =.800, p <.01). This confirms that both constructs are complements rather than substitutes.

Table 11. Descriptive statistics and bivariate correlations

Variables	JP	EXP	CI	DOING	IMPROVING	ENABLING	MANAGING
Job Position							
Experience	(.399) ***						
CI	(.125) *	.081	**.919**				
DOING	.000	.081	.450***	**.927**			
IMPROVING	.088	.016	.424***	.773***	**.890**		
ENABLING	.075	(.009)	.314***	.738***	.757***	**.909**	
MANAGING	.048	(.016)	.376***	.800***	.755***	.777***	**.936**

Notes: Correlations significant at the 0.001 level by *** and at the 0.10 level by *. Sample size = 207. In bold are the composite reliability of items. Legend: Job Position (JP), Experience (EXP), Cybersecurity Intelligence (CI).

3.5 RESULTS

Table 12 shows the results for the models with second-order variables and the dependent variable. All F-statistics are significant, and the R2 ranges from 16.3 to 24.4%. Individually, the coefficients of Doing (b = 0.450, p <0.001), Improving (b =0.438, p <0.001), Enabling (b =0.325, p <0.001), and Managing (b =0.383, p <0.001) are significantly and positively associated with CI. However, in the combinative analysis of the variables, the variable Enabling presents a negative effect that is not significant (b = -0.142, p =0.193) together with Managing (b =0.034, p =0.775), which presents a positive effect that is not significant as well. Therefore, hypothesis 1 (Managing) and hypothesis 3 (Enabling) are partially supported, and hypothesis 2 (Doing) and hypothesis 4 (Improving) are supported.

These findings translated that capabilities to build CI, from the experts' perspective, are more concerned with building, reviewing, designing, and improving cybersecurity engineering. Even though enabling and managing capabilities are relevant to the process of CI in literature (Abdul Molok et al., 2018; Ahmad et al., 2021; A. Naseer et al., 2021), our sample does not empirically demonstrate these capabilities as highly significant. These results do not corroborate other recent literature (Al-Matari et al., 2021; Brous and Janssen, 2020) that shows that management, coordination, and control provided by business leaders offer good insights into firms' available data; improving cybersecurity capabilities.

Table 12. First parameter estimates of the hierarchical linear regression for second order variables.

Variable	Model 1	Model 2	Model 3	Model 4	Model 5
Outcome	*Cybersecurity Intelligence*				
Constant	(.025) [.538]	1.026 † [.432]	1.609 *** [.453]	1.297 ** [.444]	.106 [.540]
Control Variables					
Job Position	(.127) † [.052]	(.159) * [.053]	(.138) * [.055]	(.129) * [.054]	(.143) * [.052]
Experience	(.006) [.048]	.011 [.049]	.029 [.051]	.036 [.050]	(.006) [.048]
Direct Effects					
DOING	.450*** [.118]				.315 **[.220]
IMPROVING		.438*** [.095]			.275 ** [.167]
ENABLING			.325*** [.093]		(.142) [.153]
MANAGING				.383*** [.090]	.034 [.166]
F value	14.914***	17.630***	9.389***	13.213***	10.750***
R^2	.218	.207	.122	.163	.244
R^2 Adjusted	.206***	.195***	.109***	.151***	.221***
N	203	203	203	203	203

Notes: Significance levels < 0.10 marked by †, < 0.05 by *, < 0.01 by **, <0.001 ***. Standardized coefficients. Standard errors in brackets. All VIF < or = 3.206

Many reasons may be involved in these results and must be explored more deeply in the future; however, we accept that experts are more concerned about managing cyber architectures and technologies than stakeholders and communications to deal with misunderstandings, primarily from users. Additionally, the control experience variable is not significant for CI among the models assessed. Instead, job position appears significant but negatively associated with CI. One reason for this can be related to the hierarchical organizational structure of firms, which may interfere with the agility of building innovations and cybersecurity changes, causing the decision-making process to lag (Jalali et al., 2019).

Table 13 shows additional results of regression models in a combinative way of variables. All F-statistics are significant, and the R^2 ranges from 16.5 to 23.7%. The combination of capabilities could bring new insights; thus, we analyze Doing (b = 0.278, p <0.01) and Improving (b =0.222, p <0.05), which significantly impact CI. Doing capabilities are very representative in all combinative forms with other capabilities. Improving also assumes the same importance when combined with other capabilities. The results confirm the positive and significant impact of this second-order variable on CI. However, managing (b =0.331, p <0.01) only assumes significant relevance when associated with enabling (b =0.068, p =0.509), which does not have a significant impact on CI. The isolated impact of managing as a significant capability on CI challenges us to think about its real connotation in practice. Questions on the extent to which managing capabilities impact CI have not yet been fully explained in literature (Renwick & Gleasure, 2021; Tan et al., 2016; W. Wang et al., 2019; Williams et al., 2013).

Table 13. Second parameter estimates of the hierarchical linear regression for second order variables.

Variable	Model 1	Model 2	Model 3	Model 4	Model 5	Model 6
Outcome	*Cybersecurity Intelligence*					
Constant	.095 [0.536]	1.041* [.449]	1.220 ** [.459]	(.030) [.540]	.022 [.545]	.866* [.448]
Control Variables						
Job Position	(.146) * [.052]	(.160) * [.053]	(.133) † [.054]	(.126) † [.053]	(.129) † [.052]	(.155) * [.053]
Experience	(.003) [.048]	.011 [.049]	.035 [.050]	(.006) [.049]	(.001) [.049]	.016 [.049]
Direct Effects						
DOING	.278** [.184]			.464*** [.175]	.399*** [.198]	
IMPROVING	.222* [.148]	.447*** [.145]				.343*** [.145]
ENABLING		(.012) [.135]	.068 [.144]	(.018) [.131]		
MANAGING			.331 ** [.143]		.063 [.147]	.125 [.134]
F value	15.709***	13.162***	9.992***	14.081***	14.185***	13.701***
R^2	.237	.207	.165	.218	.219	.213
R^2 Adjusted	.222***	.191***	.149***	.203***	.204***	.198***
N	202	202	202	202	202	202

Notes: Significance levels < 0.10 marked by †, < 0.05 by *, < 0.01 by **, <0.001 ***. Standardized coefficients. Standard errors in brackets. All VIF < or = 2.848.

Enabling appears with no significant impact, regardless of its positive or negative influence on CI when associated with other capabilities. One reason for this result might be in the essence of enabling establishing command and controls to facilitate timely data sharing (communication) and information management (intelligence, which involves collecting, analyzing, and disseminating the relevant information) (Cahyani et al., 2017; Diaz et al., 2019; Goles et al., 2008; Goode and Lacey, 2021). This could not have been considered by the experts as relevant in CI perhaps due to the lack of exchanging data among the experts for the sake of protecting confidentialities. Therefore, this second level of analysis corroborates the previous one, where hypothesis 1 (Managing) and hypothesis 3 (Enabling) are partially supported, and hypothesis 2 (Doing) and hypothesis 4 (Improving) are fully supported.

To clarify the effects of second-order variables, we decided to perform the third level of analysis within the composition of the first-order variables to understand their strengths in CI. Table 14 reports the results of the models of the eight first-order variables and the dependent variable. All the models' F-statistics are significant, and the R^2 ranges from 12.2 to 26.8%. Doing received more impact from ECR (b =0.210, p <.05) and RCD (b = 0.195, p <.05). Improving received more impact from IMC (b =0.419, p <.001), enabling was fully impacted by SPA (b =0.325, p <.001), and managing was significantly impacted by PMC (b =0.293, p <.01). However, in combination, only IMC (b =0.303, p <.001) presented a significant contribution to CI.

Table 14. Parameter estimates of the hierarchical linear regression for first order variables.

Variable	Model 1	Model 2	Model 3	Model 4	Model 5
Outcome	*Cybersecurity Intelligence*				
Constant	.030 * [.552]	1.265 ** [.440]	1.609 *** [.453]	1.289 ** [.443]	.334 [.553]
Control Variables					
Job Position	(.126) † [.053]	(.161) † [.052]	(.138) * [.055]	(.134) * [.054]	(.147) * [.052]
Experience	(.007) [.049]	(.003) [.048]	.029 [.051]	.040 [.050]	(.017) [.048]
Direct Effects					
ECR	.210 * [.153]				.153 [.164]
DCS	.102 [.156]				.087 [.164]
RCD	.195 * [.155]				.104 [.170]
STA		.061 [.118]			(.050) [.149]
IMC		.419*** [.104]			.303 *** [.118]
SPA			.325 *** [.093]		(.107) [.154]
PMC				.293 ** [.123]	.112 [.136]
MAS				.122 [.125]	(.042) [.141]
F value	11.296***	14.749***	9.389***	10.293***	7.163***
R^2	.219	.226	.122	.169	.268
R^2 Adjusted	.200***	.211***	.109***	.153***	.230***
N	201	202	203	202	196

Notes: Significance levels < 0.10 marked by †, < 0.05 by *, < 0.01 by **, <0.001 ***. Standardized coefficients. Standard errors in brackets. All VIF < or = 3.206

Legend: Engineering Cybersecurity Requirements (ECR); Designing Cybersecurity Solutions (DCS); Reviewing Cybersecurity Design (RCD); Standardizing Cybersecurity Activities (SCA); Improving Cybersecurity (IMC); Supporting Cybersecurity Activities (SPA); Planning & Managing Cybersecurity (PMC); Managing Stakeholders (MAS); Innovations in cybersecurity (NIC); Organizational Cybersecurity Changes (OCC); Organizational Cybersecurity Performance (OCP).

This result may be associated with the high level of activities in cybersecurity in creating processes to enhance the experimentality of security technologies, exchanging security information, providing secure communication channels to facilitate information flow, reinforcing the process of proactive and iterative detection, isolation, and mitigation of advanced threats, improving continuous security patterns following official entity recommendations, and fostering collaboration with other software development firms, among other activities (Al-Matouq et al., 2020; Goode and Lacey, 2021; Magnuson et al., 2004; H. Naseer et al., 2021; Tan et al., 2016; Wang et al., 2019). These parameters provided more details about the impact of each activity defined in our framework on CI.

3.6 DISCUSSION

Based on the consulted literature and the empirical analysis, we discuss the most important aspects of our findings. First, we find that job position and experience do not potentialize the effect of DCCI. Both are two different and unrelated constructs to CI. There is a negative correlation with job position (r = -0.125, p =0.072), and there is a positive correlation with experience (r =0.081, p =0.243) but not at a significant level, which suggests a weak

relationship. This confirms that these factors do not interfere in developing CI, conveying a message that hierarchical factors do not interfere in the process of Doing, Improving, Enabling, and Managing cybersecurity activities. It is relevant for firms to establish their cybersecurity team since the approach should not be based on positions or experiences but based on the level of capabilities.

Second, we find that Doing ($b = 0.450$, $p > 0.01$) and Improving ($b = 0.438$, $p > 0.01$) cybersecurity activities are both associated with CI at a significant level when applied in isolation or in combination [Doing ($b = 0.278$, $p > 0.01$); Improving ($b = 0.222$, $p < 0.05$)]. In other words, both capabilities are likely to be pursued by firms emphasizing development in CI because these capabilities represent a valuable part of processes and abilities to enhance organizational change to CI's achievements (Abdul Molok et al., 2018; Al-Matouq et al., 2020; Goode & Lacey, 2021).

Third, we find that Managing ($b = 0.383$, $p < .001$) is positively associated with CI individually or in combination with Enabling ($b = 0.331$, $p < 0.01$) but does not reflect any impact when combined with Doing and Improving capabilities. From a CI development standpoint, we argue that firms may prefer different cybersecurity strategies, such as experimenting with new business models or standardizing previously developed solutions (Coreynen et al., 2020; Kowalkowski et al., 2017). This may impact their level of managing and enabling capabilities for cybersecurity processes and changes. It corroborates Kapoor et al. (2021), who highlighted that it is safe to say that firms' technologies usually do not offer an end-to-end security blanket from cyber threats; therefore, firms need to consistently invest in or purchase cybersecurity services. (Kapoor et al., 2021). Abdul Molok et al. (2018) identified seven independent factors that collectively represent the managing capability to mitigate leakage. They are presented as policy integration, security education and training, technology control, security responsibility, perception, commitment to security initiatives, and employee awareness (Abdul Molok et al., 2018). Considering this study's findings considering literature, we suspect that managing and enabling are capabilities inherent for business best practices being customized according to the business requirements. This evidence provides avenues for further questions about the real connotation of these capabilities on CI, for some reasons: (1) less likely is managing and enabling activities may be absent in the business contexts investigated, (2) managing and enabling activities do not really contribute to CI, or (3) experts do not consider these activities as relevant to build CI, therefore, they do not pay attention on them.

Fourth, at the first-order construct level, we did not find a significant relation between designing cybersecurity solutions [DSR, (b =0.102, p =0.233)] and standardizing cybersecurity activities [STA, (b =0.061, p =0.450)] on CI. We suspect that a potential explanation for this result is the dynamism of process changes and innovations that affect the life cycle of software development in cybersecurity, not permitting standardization or time creation for designing projects for cybersecurity. This relates to earlier insights into how firms enable agile characteristics (flexibility, swiftness, and innovation), using key capabilities such as decision automation, on-demand and continuous data analysis and complex event processing to detect and respond to cyber incidents as they occur. This enhances overall cybersecurity performance (A. Naseer et al., 2021).

Fifth, we find that when all first-order constructs are combined, the relationships may be weakened except for improving cybersecurity [IMC, (b =0.303, p< 0.01). We understand that technological turbulence must be associated with cybersecurity intelligence, regardless of firms' emphasis on DCCI. This means that firms active in business highly dependent on technological change are more oriented toward CI development by improving their cybersecurity activities, even if they are just responding to comply with laws or regulations. They thus value cybersecurity as a way to improve existing processes when the environment offers the technological means to do so (Coreynen et al., 2020).

Finally, in terms of the connection between practice and theory about capabilities, we find that the DCCI framework is in line with prior studies, which pinpointed cybersecurity capabilities as an antecedent for the development of CI (Kolini & Janczewski, 2022). Furthermore, one of the key challenges for cybersecurity is coordinating strong planning of cybersecurity activities presented in this study as a significant capability [PMC, (b =0.293, p <0.01)]. This defines a form of governing security service level (confidentiality and partners agreements, hierarchical structure of roles and responsibilities) by using flat and flexible organizational structures to maintain security activities and develop and implement an action plan to fulfill security maturity criteria (Ahmad et al., 2021; Akinsanya et al., 2019; Goode & Lacey, 2021). Therefore, our DCCI framework toward improving cybersecurity capabilities also corroborates Akinsanya et al. (2019), who highlighted that maturity models provide a structure for improving firms' capabilities; although several cybersecurity maturity models and standards resolving specific threats exist, there is still a lack of maturity models available (Akinsanya et al., 2019).

3.7 CONCLUSION

This study answered the research question that having cybersecurity capabilities enables firms to build their CI. However, not all capabilities directly impact CI development, and an appropriately identifying the needed process and abilities for cybersecurity business requirements is necessary. We also demonstrate that the capabilities indicated in our framework may be considered dynamic capabilities because of their influence in changing and performing CI and how they are classified according to dynamic capability microfoundations. Our findings reveal the relevance of cybersecurity engineering and improvements in cybersecurity activities to develop CI. It also pointed out that managing cybersecurity is more relevant in planning activities to adjust team structure to business requirements.

3.7.1 Theoretical Contribution

Despite the increasing attention to building cybersecurity capabilities (Al-Matouq et al., 2020; Srivatanakul & Annansingh, 2021), literature does not fully explore the factors that drive firms to develop a DCCI. Therefore, we conceptualized dynamic capabilities in cybersecurity as processes and abilities to identify, mobilize, and renew resources against cyber fraud to impact CI in firms. To date, literature has focused on understanding the security field by obtaining qualification through certifications and technical aptitude (Srivatanakul & Annansingh, 2021). Cybersecurity professionals usually perform functions applying continuous network monitoring, troubleshooting, and providing real-time security solutions. However, even with all efforts applied to a combination of capabilities that enables a person to do something well (Boyatzis & Kolb, 1991; Carlton et al., 2019), analytical skills and soft skills surrounding the hardware and software are required to enhance CI to mitigate cyberattacks (Carlton et al., 2019).

The cybersecurity capabilities literature still lacks the theoretical foundation to explain what are the effective capabilities that should be evidenced as dynamic capabilities. Therefore, this study offers new insights into literature by investigating DCCI drivers from both an internal perspective [i.e., dynamic capabilities; (Teece, 2007)] and an external perspective [i.e., fraud diamond theory; (Wolfe & Hermanson, 2004)].

Concerning the impact of DCCI as an internal driver, we find that both Doing and Improving are positively associated with firms pursuing a CI. Depicting the process of systems architecture (physical, electronic relationships), establishing infrastructure (mechanisms and

processes), validating security mechanisms, and seeking analytical information are useful DCCIs to turn CI into a success (Attili et al., 2018; Bartnes & Moe, 2017; Cahyani et al., 2017; Diaz et al., 2019; Goode & Lacey, 2021). Without DCCI to refine current or adopt breakthrough technologies, firms are less likely to change their cybersecurity strategy by building CI. This makes firms vulnerable to cyberattacks, for example, new networks that demand shifting technologies may jeopardize the data chain beyond further heterogeneous demands to address business requirements.

Concerning the impact of DCCI as an external driver, we find that enabling and managing does not significantly impact CI, as seen in literature (Abdul Molok et al., 2018; Ahmad et al., 2021; Attili et al., 2018). The context in which firms operate does matter (Dmitrijeva et al., 2020), and they deal with cyberattacks differently depending on their maturity in the DCCI. For instance, we find that firms are more likely to pursue CI when the technology in their sector is vulnerable. One of the respondents provided us with an additional comment in the survey*: "Currently, C-levels and above are only concerned with data protection laws because the fines for noncompliance are very high; however, this same engagement is not observed because we still have high-profile people, company executives, who regard information security as an unnecessary expense*". This evidence corroborates Teece et al. (1997), who highlighted that firms would adjust their strategy not only depending on their dynamic capabilities but also on the environment in which they are active (Teece, 2007).

Therefore, looking into CI from a dynamic capabilities lens offered a multidimensional perspective of firms' strategic transition. For example, another respondent stated that "*It is important to consider a top-down approach for cyber security awareness that leads to a proper risk appetite in the leadership team and drives a consistent increase on budgeting and fundamentals for new acquisitions in terms of tools and information systems policies*". Hence, this influence of managing and enabling cybersecurity activities to create CI is associated with the business environment and practices, recognized as cybersecurity capabilities or business capabilities inherent in leadership practices. In summary, this study contributes to literature by pinpointing a DCCI framework for CI (Kolini & Janczewski, 2022), as well as the influence of having a more aggregate impact on managing and enabling capabilities.

3.7.2 Managerial implications

From a business perspective, this study captures "*appropriate parameters and data points*", as mentioned by one of the respondents. Based on this study's results, we offer several

implications for managers. Most notably, we highlight the importance of developing DCCI to develop CI in general. This can be accomplished by actively engineering cybersecurity requirements (ECR); designing cybersecurity solutions (DCS); reviewing cybersecurity design (RCD); standardizing cybersecurity activities (SCA); improving cybersecurity (IMC); supporting cybersecurity activities (SPA); planning and managing cybersecurity (PMC); managing stakeholders (MAS) for innovations in cybersecurity (NIC); organizational cybersecurity changes (OCC); and organizational cybersecurity performance (OCP). For example, one of the respondents pointed out that "*this survey is very insightful and gave some very good perspectives".* Another interviewee mentioned, "*I was wondering if I could borrow this from you for internal use*" or yet "*most global advisory companies do not ask questions that are as relevant and material as this survey*". In practice, this means that firms must frequently adjust their capabilities and procedures to improve their accuracy and efficiency in developing CI; therefore, researchers must be aware of creating time to discuss and experiment with new ideas that challenge conventional wisdom.

Without developing a DCCI framework, firms are likely unable to adapt their strategy to the increasingly process developing CI. Furthermore, as mentioned by another respondent, "*intelligence sharing is important, especially from the industry that is in the same line of business as your organization. Security is evolving, and hence, continuous review and adaptability to the threat landscape are paramount*". In this vein, by developing DCCI, firms are more likely to consider the changes in the environment in which they are networking. This study shows that when there is development in the DCCI, firms are more likely to be less vulnerable, especially if they are focused on cyberattacks, and this seems to be obvious, but it is not, considering that neglected behaviors still exist in corporate environments. Therefore, we suggest that firms pay close attention to their networks and technological environments to develop a DCCI framework that is even more effective in adapting to highly evolving CI.

3.7.3 Limitations and suggestions for future research

This study has some limitations. First, the variables for DCCI and CI may offer limited insights into the drivers of information security. Second, although one of the first to contribute empirically to the theoretical underpinnings of capabilities in cybersecurity, this study provides data from a single survey completed by multiple respondents. Third, even using several techniques when developing the survey to prevent the endogeneity of the variables, the

instrument applied does not capture all capabilities for cybersecurity. Fourth, DCCI and CI are based on literature developed by practitioners and case-study findings, and the measures are open to interpretation and might not reflect the actual rate of DCCI.

As opportunities for further research, a potentially fruitful next step is to consider additional DCCI or review them into the model or add measures involving CI to permit information security managers to play on "how" capabilities effectively control the endpoint complexity that does not hurt innovations (Jalali et al., 2019). Future studies could also question more about managing external stakeholders and validating these capabilities in the model, especially those firms providing IT services. Additionally, quantifying all variables more rigorously could improve this model.

3.8 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

ACFE. (2022). Occupational Fraud 2022: A Report to the nations [Report to the Nations on Occupational Fraud and Abuse]. Association Certified Fraud Examiners. https://legacy.acfe.com/report-to-the-nations/2022/

Aharoni, E., Peleg, R., Regev, S., & Salman, T. (2016). Identifying malicious activities from system execution traces. IBM Journal of Research and Development, 60(4), 5:1-5:7. https://doi.org/10.1147/JRD.2016.2559358

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

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 Jallad, K., Aljnidi, M., & Desouki, M. S. (2020). Anomaly detection optimization using big data and deep learning to reduce false-positive. Journal of Big Data, 7(1), 68. https://doi.org/10.1186/s40537-020-00346-1

Albrecht, W. S., Albrecht, C., & Albrecht, C. C. (2008). Current Trends in Fraud and its Detection. Information Security Journal: A Global Perspective, 17(1), 2–12. https://doi.org/10.1080/19393550801934331

Al-Matari, O. M. M., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2021). Adopting security maturity model to the organizations' capability model. Egyptian Informatics Journal, 22(2), 193–199. https://doi.org/10.1016/j.eij.2020.08.001

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

Amrein, A., Angeletti, V., Beitler, A., Nemet, M., Reiser, M., Riccetti, S., Stoecklin, M. Ph., & Wespi, A. (2016). Security intelligence for industrial control systems. IBM Journal of Research and Development, 60(4), 13:1-13:12. https://doi.org/10.1147/JRD.2016.2575698

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. Journal of Systems and Information Technology, 21(1), 2–35. https://doi.org/10.1108/JSIT-02-2018-0028

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

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

Berger, S., Garion, S., Moatti, Y., Naor, D., Pendarakis, D., Shulman-Peleg, A., Rao, J. R., Valdez, E., & Weinsberg, Y. (2016). Security intelligence for cloud management infrastructures. IBM Journal of Research and Development, 60(4), 11:1-11:13. https://doi.org/10.1147/JRD.2016.2572462

Boyatzis, R. E., & Kolb, D. A. (1991). Assessing Individuality in Learning: The learning skills profile. Educational Psychology, 11(3–4), 279–295. https://doi.org/10.1080/0144341910110305

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

Brous, P., & Janssen, M. (2020). Trusted Decision-Making: Data Governance for Creating Trust in Data Science Decision Outcomes. Administrative Sciences, 10(4), 81. https://doi.org/10.3390/admsci10040081

Brown, S., Gommers, J., & Serrano, O. (2015). From Cyber Security Information Sharing to Threat Management. Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, 43–49. https://doi.org/10.1145/2808128.2808133

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

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

Carlton, M., Levy, Y., & Ramim, M. (2019). Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. Information & Computer Security, 27(1), 101–121. https://doi.org/10.1108/ICS-11-2016-0088

Chari, S. N., Habeck, T. A., Molloy, I., Park, Y., Rao, J. R., & Teiken, W. (2016). A platform and analytics for usage and entitlement analytics. IBM Journal of Research and Development, 60(4), 7:1-7:12. https://doi.org/10.1147/JRD.2016.2560558

Cieslewicz, J. K. (2012). The fraud model in international contexts: A call to include societal-level influences in the model. Journal of Forensic and Investigative Accounting, 4(1), 214–254. http://web.nacva.com.s3.amazonaws.com/JFIA/Issues/JFIA-2012-1_8.pdf

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

Coden, A., Lin, W. S., Houck, K., Tanenblatt, M., Boston, J., MacNaught, J. E., Soroker, D., Weisz, J. D., Pan, S., Lai, J.-H., Lu, J., Wood, S., Xia, Y., & Lin, C.-Y. (2016). Uncovering insider threats from the digital footprints of individuals. IBM Journal of Research and Development, 60(4), 8:1-8:11. https://doi.org/10.1147/JRD.2016.2568538

Coreynen, W., Matthyssens, P., Vanderstraeten, J., & van Witteloostuijn, A. (2020). Unravelling the internal and external drivers of digital servitization: A dynamic capabilities and contingency perspective on firm strategy. Industrial Marketing Management, 89, 265–277. https://doi.org/10.1016/j.indmarman.2020.02.014

Dalziel, H., Olson, E., & Carnall, J. (2015). How to define and build an effective cyber threat intelligence capability. Syngress is an imprint of Elsevier. http://www.books24x7.com/marc.asp?bookid=78688

Dani, M. V., & Gandhi, A. V. (2021). Understanding the drivers of innovation in an organization: A literature review. International Journal of Innovation Science. https://doi.org/10.1108/IJIS-10-2020-0201

Daryanto, A. (2020). EndoS: An SPSS macro to assess endogeneity. The Quantitative Methods for Psychology, 16(1), 56–70. https://doi.org/10.20982/tqmp.16.1.p056

Dellios, K., Papanikas, D., & Polemi, D. (2015). Information Security Compliance over Intelligent Transport Systems: Is IT Possible? IEEE Security & Privacy, 13(3), 9–15. https://doi.org/10.1109/MSP.2015.59

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

Diesch, R., Pfaff, M., & Krcmar, H. (2018). Prerequisite to Measure Information Security—A State of the Art Literature Review: Proceedings of the 4th International Conference on Information Systems Security and Privacy, 207–215. https://doi.org/10.5220/0006545602070215

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. Computers & Security, 92, 101747. https://doi.org/10.1016/j.cose.2020.101747

Dmitrijeva, J., Schroeder, A., Ziaee Bigdeli, A., & Baines, T. (2020). Context matters: How internal and external factors impact servitization. Production Planning & Control, 31(13), 1077–1097. https://doi.org/10.1080/09537287.2019.1699195

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

Elmo, G. C., Arcese, G., Valeri, M., Poponi, S., & Pacchera, F. (2020). Sustainability in Tourism as an Innovation Driver: An Analysis of Family Business Reality. Sustainability, 12(15), 6149. https://doi.org/10.3390/su12156149

Elragal, A., & Haddara, M. (2012). The Future of ERP Systems: Look backward before moving forward. Procedia Technology, 5, 21–30. https://doi.org/10.1016/j.protcy.2012.09.003

Ferrando, P. J., & Lorenzo-Seva, U. (2017). Program FACTOR at 10: Origins, development and future directions. Psicothema, 29.2, 236–240. https://doi.org/10.7334/psicothema2016.304

Ferrando, P. J., & Lorenzo-Seva, U. (2018). Assessing the Quality and Appropriateness of Factor Solutions and Factor Score Estimates in Exploratory Item Factor Analysis. Educational and Psychological Measurement, 78(5), 762–780. https://doi.org/10.1177/0013164417719308

Garcia-Perez, A., Sallos, M. P., & Tiwasing, P. (2021). Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: An intellectual capital perspective. Journal of Intellectual Capital. https://doi.org/10.1108/JIC-06-2021-0166

Gibson Jr., T. O., Morrow, J. A., & Rocconi, L. M. (2020). A Modernized Heuristic Approach to Robust Exploratory Factor Analysis. The Quantitative Methods for Psychology, 16(4), 295–307. https://doi.org/10.20982/tqmp.16.4.p295

Gill, M. (2011). Fraud and recessions: Views from fraudsters and fraud managers. International Journal of Law, Crime and Justice, 39(3), 204–214. https://doi.org/10.1016/j.ijlcj.2011.05.008

Gkoulalas-Divanis, A., & Braghin, S. (2016). IPV: A system for identifying privacy vulnerabilities in datasets. IBM Journal of Research and Development, 60(4), 14:1-14:10. https://doi.org/10.1147/JRD.2016.2576818

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., & 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

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2009). Análise multivariada de dados (6o ed). Bookman. https://books.google.com/books?id=oFQs_zJI2GwC

Harerimana, A., & Mtshali, N. G. (2020). Using Exploratory and Confirmatory Factor Analysis to understand the role of technology in nursing education. Nurse Education Today, 92, 104490. https://doi.org/10.1016/j.nedt.2020.104490

Hausman, J. A. (1978). Specification Tests in Econometrics. Econometrica, 46(6), 1251. https://doi.org/10.2307/1913827

Horne, C. A., Maynard, S. B., & Ahmad, A. (2017). Organisational Information Security Strategy: Review, Discussion and Future Research. Australasian Journal of Information Systems, 21. https://doi.org/10.3127/ajis.v21i0.1427

Howard, M. C. (2016). A Review of Exploratory Factor Analysis Decisions and Overview of Current Practices: What We Are Doing and How Can We Improve? International Journal of Human-Computer Interaction, 32(1), 51–62. https://doi.org/10.1080/10447318.2015.1087664

Hu, X., Jang, J., Wang, T., Ashraf, Z., Stoecklin, M. Ph., & Kirat, D. (2016). Scalable malware classification with multifaceted content features and threat intelligence. IBM Journal of Research and Development, 60(4), 6:1-6:11. https://doi.org/10.1147/JRD.2016.2559378

Ikeda, K., Marshall, A., & Zaharchuk, D. (2019). Agility, skills and cybersecurity: Critical drivers of competitiveness in times of economic uncertainty. Strategy & Leadership, 47(3), 40–48. https://doi.org/10.1108/SL-02-2019-0032

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

Jasper, S. E. (2017). U.S. Cyber Threat Intelligence Sharing Frameworks. International Journal of Intelligence and CounterIntelligence, 30(1), 53–65. https://doi.org/10.1080/08850607.2016.1230701

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

Karimi, J., & Walter, Z. (2015). The Role of Dynamic Capabilities in Responding to Digital Disruption: A Factor-Based Study of the Newspaper Industry. Journal of Management Information Systems, 32(1), 39–81. https://doi.org/10.1080/07421222.2015.1029380

Karimi, J., & Walter, Z. (2021). The Role of Entrepreneurial Agility in Digital Entrepreneurship and Creating Value in Response to Digital Disruption in the Newspaper Industry. Sustainability, 13(5), 2741. https://doi.org/10.3390/su13052741

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

Kosutic, D., & Pigni, F. (2022). Cybersecurity: Investing for competitive outcomes. Journal of Business Strategy, 43(1), 28–36. https://doi.org/10.1108/JBS-06-2020-0116

Kowalkowski, C., Gebauer, H., & Oliva, R. (2017). Service growth in product firms: Past, present, and future. Industrial Marketing Management, 60, 82–88. https://doi.org/10.1016/j.indmarman.2016.10.015

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, Y., & Okui, R. (2012). Hahn–Hausman test as a specification test. Journal of Econometrics, 167(1), 133–139. https://doi.org/10.1016/j.jeconom.2011.10.005

Li, Q., Lan, L., Zeng, N., You, L., Yin, J., Zhou, X., & Meng, Q. (2019). A Framework for Big Data Governance to Advance RHINs: A Case Study of China. IEEE Access, 7, 50330–50338. https://doi.org/10.1109/ACCESS.2019.2910838

Li, Y.-H., & Huang, J.-W. (2013). Exploitative and exploratory learning in transactive memory systems and project performance. Information & Management, 50(6), 304–313. https://doi.org/10.1016/j.im.2013.05.003

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

Malatji, M., Marnewick, A. L., & Von Solms, S. (2022). Cybersecurity capabilities for critical infrastructure resilience. Information & Computer Security, 30(2), 255–279. https://doi.org/10.1108/ICS-06-2021-0091

Mansor, R. A. N. (2015). Forensic accounting and fraud risk factors: The influence of fraud diamond theory. The American Journal of Innovative Research and Applied Sciences, 7(28), 186–192. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.695.8486&rep=rep1&type=pdf

Marinho, M., Prakash, V., Garg, L., Savaglio, C., & Bawa, S. (2021). Effective Cloud Resource Utilisation in Cloud ERP Decision-Making Process for Industry 4.0 in the United States. Electronics, 10(8), 959. https://doi.org/10.3390/electronics10080959

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

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

Mishra, P., Yadav, S. K., Sachdeva, R. K., & Kishor, A. (2022). Novel lightweight interactive IoT end device architecture with tight security intelligence confidentiality, integrity, authenticity and availability. International Journal of System Assurance Engineering and Management, 13(S1), 212–224. https://doi.org/10.1007/s13198-021-01369-4

Mtsweni, J. S., Shozi, N. A., Matenche, K., Mutemwa, M., Mkhonto, N., & Jansen van Vuuren, J. (2016). Development of a semantic-enabled cybersecurity threat intelligence sharing model. ResearchSpace. http://hdl.handle.net/10204/9370

Mutemwa, M., Mtsweni, J., & Mkhonto, N. (2017). Developing a cyber threat intelligence sharing platform for South African organisations. 2017 Conference on Information Communication Technology and Society (ICTAS), 1–6. https://doi.org/10.1109/ICTAS.2017.7920657

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

Orlikowski, W. J., & Iacono, C. S. (2001). Research Commentary: Desperately Seeking the "IT" in IT Research—A Call to Theorizing the IT Artifact. Information Systems Research, 12(2), 121–134. https://doi.org/10.1287/isre.12.2.121.9700

Pigola, A., & Da Costa, P. R. (2021). Intellectual Dynamics: A future for dynamic capabilities and Intellectual Capital. International Journal of Development Research, 11(6), 48047–48055. https://doi.org/10.37118/ijdr.22180.06.2021

Pigola, A., & da Costa, P. R. (2023). Dynamic Capabilities in Cybersecurity Intelligence: A Meta-Synthesis to Enhance Protection Against Cyber Threats. Communications of the Association for Information Systems, 53(1), 46. Retrieved from https://aisel.aisnet.org/cais/vol53/iss1/46

Qiang, L., Zeming, Y., Baoxu, L., Zhengwei, J., & Jian, Y. (2017). Framework of Cyber Attack Attribution Based on Threat Intelligence. Em N. Mitton, H. Chaouchi, T. Noel, T. Watteyne, A. Gabillon, & P. Capolsini (Orgs.), Interoperability, Safety and Security in IoT (Vol. 190, p. 92–103). Springer International Publishing. https://doi.org/10.1007/978-3-319-52727-7_11

Queiroz, M., Tallon, P. P., Sharma, R., & Coltman, T. (2018). The role of IT application orchestration capability in improving agility and performance. The Journal of Strategic Information Systems, 27(1), 4–21. https://doi.org/10.1016/j.jsis.2017.10.002

Ramamoorti, S., Morrison, D., & Koletar, J. W. (2009). Bringing Freud to Fraud: Understanding the state-of-mind of the C-level suite/white collar offender through "ABC" analysis. Institute for Fraud Prevention (IFP) at West Virginia University. https://ecommons.udayton.edu/acc_fac_pub/71/

Rao, J. R. (2016). Preface: Security intelligence. IBM Journal of Research and Development, 60(4), 0:1-0:5. https://doi.org/10.1147/JRD.2016.2577366

Rao, J. R., Chari, S. N., Pendarakis, D., Sailer, R., Stoecklin, M. Ph., Teiken, W., & Wespi, A. (2016). Security 360°: Enterprise security for the cognitive era. IBM Journal of Research and Development, 60(4), 1:1-1:13. https://doi.org/10.1147/JRD.2016.2556958

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

Robinson, N., & Disley, E. (2010). Incentives and challenges for information sharing in the context of network and information security. European Network and Information Security Agency (ENISA).

Rustiarini, N. W., T., S., Nurkholis, N., & Andayani, W. (2019). Why people commit public procurement fraud? The fraud diamond view. Journal of Public Procurement, ahead-of-print(ahead-of-print). https://doi.org/10.1108/JOPP-02-2019-0012

Saluja, S., Aggarwal, A., & Mittal, A. (2021). Understanding the fraud theories and advancing with integrity model. Journal of Financial Crime. https://doi.org/10.1108/JFC-07-2021-0163

Schales, D. L., Jang, J., Wang, T., Hu, X., Kirat, D., Wuest, B., & Stoecklin, M. Ph. (2016). Scalable analytics to detect DNS misuse for establishing stealthy communication channels. IBM Journal of Research and Development, 60(4), 3:1-3:14. https://doi.org/10.1147/JRD.2016.2557639

Schryen, G. (2015). Writing Qualitative IS Literature Reviews—Guidelines for Synthesis, Interpretation, and Guidance of Research. Communications of the Association for Information Systems, 37. https://doi.org/10.17705/1CAIS.03712

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

Serrano, O., Dandurand, L., & Brown, S. (2014). On the Design of a Cyber Security Data Sharing System. Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security - WISCS '14, 61–69. https://doi.org/10.1145/2663876.2663882

Sharma, S., Mukherjee, S., Kumar, A., & Dillon, W. R. (2005). A simulation study to investigate the use of cutoff values for assessing model fit in covariance structure models. Journal of Business Research, 58(7), 935–943. https://doi.org/10.1016/j.jbusres.2003.10.007

Sprong, N., Driessen, P. H., Hillebrand, B., & Molner, S. (2021). Market innovation: A literature review and new research directions. Journal of Business Research, 123, 450–462. https://doi.org/10.1016/j.jbusres.2020.09.057

Srivatanakul, T., & Annansingh, F. (2021). Incorporating active learning activities to the design and development of an undergraduate software and web security course. Journal of Computers in Education, 0123456789. https://doi.org/10.1007/s40692-021-00194-9

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

Stock, J. H., & Watson, M. W. (2019). Introduction to econometrics. Pearson.

Stoecklin, M. Ph., Singh, K., Koved, L., Hu, X., Chari, S. N., Rao, J. R., Cheng, P.-C., Christodorescu, M., Sailer, R., & Schales, D. L. (2016). Passive security intelligence to analyze the security risks of mobile/BYOD activities. IBM Journal of Research and Development, 60(4), 9:1-9:13. https://doi.org/10.1147/JRD.2016.2569858

Tabachnick, B. G., & Fidell, L. S. (2014). Using multivariate statistics. https://ebookcentral.proquest.com/lib/anu/detail.action?docID=5175291

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

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

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber-attacks. Computers & Security, 72, 212–233. https://doi.org/10.1016/j.cose.2017.09.001

Townsend, T., Ludwick, M., McAllister, J., Mellinger, A. O., & Sereno, K. A. (2013). SEI emerging technology center: Cyber intelligence tradecraft project-summary of key findings. Software Engineer Institute: Carnegie Melon.

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems, 28(2), 118–144. https://doi.org/10.1016/j.jsis.2019.01.003

Vogel, R. (2016). Closing the Cybersecurity Skills Gap. Salus Journal, 4(2), 32–46.

Vousinas, G. L. (2019). Advancing theory of fraud: The S.C.O.R.E. model. Journal of Financial Crime, 26(1), 372–381. https://doi.org/10.1108/JFC-12-2017-0128

Wang, G., Dou, W., Zhu, W., & Zhou, N. (2015). The effects of firm capabilities on external collaboration and performance: The moderating role of market turbulence. Journal of Business Research, 68(9), 1928–1936. https://doi.org/10.1016/j.jbusres.2015.01.002

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

Wang, W. Y. C., Pauleen, D. J., & Zhang, T. (2016). How social media applications affect B2B communication and improve business performance in SMEs. Industrial Marketing Management, 54, 4–14. https://doi.org/10.1016/j.indmarman.2015.12.004

Wei, H.-L., & Wang, E. T. G. (2010). The strategic value of supply chain visibility: Increasing the ability to reconfigure. European Journal of Information Systems, 19(2), 238–249. https://doi.org/10.1057/ejis.2010.10

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

Wollack, J. A., Cohen, A. S., & Wells, C. S. (2003). A Method for Maintaining Scale Stability in the Presence of Test Speededness. Journal of Educational Measurement, 40(4), 307–330. https://doi.org/10.1111/j.1745-3984.2003.tb01149.x

3.9 APPENDIX E. FACTOR ANALYSIS RESULTS OF THE CONSTRUCTS

2nd Order	1st Order	Code	Questions	Loadings DDCY	Loadings CI	AVE	CR	ᾱ
Doing	Engineering Cybersecurity Requirements	ECR1	We have an information security technological architecture compatible to our existing processes, practices, and systems.	**.639**	-.001	.782	.798	.943
		ECR2	We constantly modernize our technological infrastructure to anticipate to new information security technologies	**.617**	.107			
		ECR3	We have established and documented path of our cyber defense	**.743**	-.032			
		ECR4	We use automation from external security solutions and / or technologies associated in our information security architecture	**.463**	.171			
	Designing Cybersecurity Solutions	DCS1	We have an implemented process to information security tools changes when necessary	**.522**	.099	.759	.761	.939
		DCS2	Potential customers' reactions and stakeholders' ideas are considered to create and/or use a new information security solution.	**.508**	.069			
		DCS3	We consider market security best practices systematically in our information security projects.	**.569**	.051			
		DCS4	We consider our previous experiences in information security to support our decision-making in designing security practices and tools	**.715**	-.115			
	Reviewing Cybersecurity Design	RCD1	We validate our security mechanisms and procedures on regular basis	**.652**	.116	.778	.852	.941
		RCD2	We check our technology readiness to ensure a secure work environment	**.702**	.053			
		RCD3	We use technical support of partners to review our security mechanisms and procedures	**.531**	-.049			
		RCD4	We analyze security threats and incidents from multiple internal and external sources of data	**.641**	.095			
		RCD5	We regularly review our cyber crisis or incident response plan	**.687**	.056			
Improving	Standardizing Cybersecurity Activities	STA1	We implement data security measures easily	**.712**	-.110	.832	.862	.938
		STA2	We embed information security practices and protocols within business operations easily	**.679**	-.027			
		STA3	Our information security procedures are recognized by our security policy standardization	**.746**	-.103			
		STA4	Proven security tools are used to manage and prevent our cyber-risks	**.636**	.047			
	Improving Cybersecurity	IMC1	We simulate breaches in our security authority levels to validate our cybersecurity protocols	**.556**	.160	.736	.723	.939
		IMC2	We have proactive and iterative detection and mitigation of advanced threats that are not detected by traditional security controls	**.667**	.024			
		IMC3	We usually attempt or experiment new security tools in course of developing to acquire new outcomes	**.512**	.215			
		IMC4	We collaborate with other software development firms to improve our security requirements	**.446**	.192			
Enabling	Supporting Cybersecurity Activities	SPA1	We have adequate security capacity to monitor teams' activities	**.728**	.008	.874	.909	.938
		SPA2	We provide technical support for the adoption of adequate security measures.	**.704**	-.066			
		SPA3	We have effective mechanisms in place for identification of risks and threats for our data	**.828**	-.147			

		SPA4	In an event of an information security incident, we have efficient mechanisms in place for external communication to potentially affected parties	**.802**	-.095			
Managing	Planning & Managing Cybersecurity	PMC1	We disclosure of security risk measures to the organization racking from key indicators	**.773**	-.074	.839	.871	.938
		PMC2	We have a risk management program based on recognized security standards	**.739**	-.047			
		PMC3	We have a hierarchical structure of roles and responsibilities for different security service levels	**.708**	-.007			
		PMC4	We use data analytics driven decision-making to develop a firmer tone of our security management intent	**.603**	.135			
	Managing Stakeholders	MAS1	Regular trainings keep our stakeholders able to make correct decisions to protect our information from cyber-attacks	**.666**	-.049	.778	.886	.938
		MAS2	Through security risk assessment, we empower the decision makers to take the appropriate timely action in case of cyber incidents	**.747**	-.022			
		MAS3	We have clear guidelines around what is our cyber risk tolerance	**.747**	-.022			
		MAS4	Our senior managers play a pivotal role in spreading formal cybersecurity education.	**.650**	.063			
		MAS5	Our management board has a sufficient understanding of the digital technologies threats to our organization	**.651**	.011			
Cybersecurity Intelligence	Innovation, change and perform	NIC1	In the last 12 months, the number of new information security technologies implemented or experimented was… (1-2;3-4;5-6;7-9;above 10)	-.175	**.900**	.778	.919	.938
		NIC2	In the last 12 months, the number of new information security processes developed, implemented, or experimented was… (1-2;3-4;5-6;7-9;above 10)	-.199	**.972**			
		OCC1	In the last 12 months, the number of new security controls proactively implemented was…(1-2;3-4;5-6;7-9;above 10)	-.212	**.905**			
		OCC2	In the last 12 months, The number of information security data sources in our network increased in... (Less than 5%; 6% – 10%; 11% – 15%; 15% – 20%; above 21%)	-.018	**.449**			
		OCP1	In the last 12 months, the number of identified new security threat-actors highlighting gaps in our cyber defenses was... (1-2;3-4;5-6;7-9;above 10)	-.085	**.532**			

Note. EFA = Exploratory Factor Analysis. Extraction method: Parallel Analysis. Rotation method: Robust Promin; RMSEA = 0.062, p = .05; Barlett Test 2,223.9 (741); p < .001; Kaiser-Meyer-Olkin (KMO) test = . 938; Factor explained 48.02% of variance. A significance test is performed using a bootstrapping procedure with 500 subsamples.

4 STUDY 3. ENHANCING CYBERSECURITY CAPABILITIES INVESTMENTS: EVIDENCE FROM AN EXPERIMENT

In recent years, investments in cybersecurity capabilities (CC) have emerged as an essential practice in reducing cyberattacks and optimizing the usage of technologies. Therefore, optimal investments in capabilities must be determined according to the cybersecurity scenario of firms. This experiment pursues an understanding of the effectiveness of the iterative learning process in investments in CC . Through a simulator game, experienced and inexperienced participants overcome challenges related to uncertainties of cyber incidents to decision-making in cybersecurity capability investments. The collected data were empirically tested from 119 participants analyzing 3,808 simulation runs. The findings demonstrated that there is a slight difference in the learning curve between the two groups even if they learn proactively and iteratively. However, experienced, and inexperienced groups did not demonstrate enough capacity to analyze the cybersecurity ecosystems designed in the simulator game to mitigate cyber incidents. Both groups exhibited similar results regarding gaps to invest in CC to address uncertainties associated with cyber threats. In this sense, this experiment highlights the relevance of learning about CC investments in any context to avoid resource losses and time to uncover the complexities related to incident responses.

4.1 INTRODUCTION

Cyberattacks tend to pose an ongoing threat as they become increasingly sophisticated, and firms invest in cybersecurity based on their cybersecurity capabilities (CC) and experienced cyberattacks (Fernandez De Arroyabe et al., 2023). A decade ago, cybersecurity was a matter of "if" a company would be affected or compromised, but currently it is a matter of "when" and "at what level" (D'Arcy et al., 2020; Jalali et al., 2019; Kour & Karim, 2020). Critical cyberattacks and data breaches that have been affecting firms around the world reveal how relevant it is for firms to remain active and vigilant to protect against cyber incidents (Fleischman et al., 2023). Therefore, cybersecurity investment is a strategic decision in organizations (Fernandez De Arroyabe et al., 2023; Gupta et al., 2021). For example, firms have adapted information technologies to cope with the challenges of the current cybersecurity threats. According to the IBM Security report, the average cost of a data breach reached an all-time high of USD 4.45 million in 2023. This represents a 2.3 percent increase from the 2022 cost of USD 4.35 million. Thus, 51 percent of 553 organizations analyzed are planning to increase security investments as a result of a breach (IBM Security, 2023). Furthermore, data

breach costs and identification sources are antecedents to cybersecurity investment decisions (Shaikh & Siponen, 2023).

However, beyond financial impact (Cavusoglu et al., 2004), cyber-attacks may cause irreparable harm to firms in the form of corporate liability (Chellappa & Pavlou, 2002), promoting weakened competitive positions and promoting profitability and credibility losses (Crossler et al., 2013; Jalali & Kaiser, 2018; Kalderemidis et al., 2022). Additionally, while data breach costs continue to rise, firms are challenged whether they plan to increase investments and in which areas they must identify for additional investments (IBM Security, 2023). Therefore, executives, entrepreneurs, and IT specialists must overcome the gap on which capabilities to invest to aim cyber protection. The relevance of being prepared and proactively engaged in building CC is more cost-effective than taking a reactive approach when cyberattacks have already occurred (Adams & Makramalla, 2015; Benz & Chatterjee, 2020; Kwon & Johnson, 2014). While many firms are already aware of the importance of cybersecurity, a large number of small and medium businesses remain out of date on the main cybersecurity requirements and resources to protect them from hackers (Benz & Chatterjee, 2020; Kabanda et al., 2018). Then, they need accurate knowledge to redirect investments and efforts $in\ CC$ development. Furthermore, as data exchange and technologies grow in size and value, cyber-risks and privacy concerns demand improvements in different directions, and investments in capability development are crucial due to interventions to build improvements in technological legacy and purchase of new technologies (Jalali et al., 2019; L. Xu et al., 2023).

In this vein, this experiment addresses these challenges and gaps, demonstrating the benefits of iterative learning on how to invest in CC a cyber scenario of threats and promoting insights to overcome cyber-risks and security requirements to demystify the complexity around the theme. Academics have investigated investments in cybersecurity under a simulation approach (Fernandez De Arroyabe et al., 2023; Gupta et al., 2021; Jalali et al., 2019; Master et al., 2022); however, the learning curve of participants has not been emphasized or investigated in depth. Hence, our research motivation is to identify how experienced and inexperienced individuals react and learn to invest in CC under an uncertain scenario of cyber incidents (Catota et al., 2019; Dhillon et al., 2021). It promotes an opportunity for the virtual educative learning process to be applied in different context-specifics. In this way, two research questions are posited:

RQ1. Are there differences between experienced and inexperienced groups in investing in cybersecurity capability?

RQ2. Can the learning process in cybersecurity capability investments be achieved through a virtual iterative environment?

The experiment contributes by presenting three different groups of capabilities in cybersecurity, such as doing (CC_D), enabling (CC_E), and improving (CC_I) represented in a fictitious firm scenario. It helps to understand how experienced and inexperienced groups behave under a cybersecurity ecosystem to bring further foundations about barriers to learning in CC investments. Through an examination of the effects on capability investments around uncertainties scenario, it still purses to emphasize the effects of iterative learning as a powerful process to enhance cybersecurity posture (Master et al., 2022). It applies a systematic approach using system dynamics modeling already used in previous experiments (Hwang & Helser, 2022; Jalali et al., 2019; Khalid Khan et al., 2022; Meland et al., 2019) by visualizing the issue of investments, including impacts of delays and their consequences.

In summary, the goal of this experiment is to examine differences in the learning curve of experienced and inexperienced groups on investing in CC when they are at cyber-risk pressure. In analyzing 3,808 simulation runs a sample of events, the results indicated there is a slight difference in the learning process between both groups even if they learn proactively and iteratively. In terms of risks inherent in a cybersecurity ecosystem, we find that both groups did not demonstrate enough capacity to analyze the cybersecurity ecosystem designed in the simulator to mitigate cyber incidents through accurate investments. In addition, the results indicated that trust in the simulator positively impacted the effectiveness of the experiment.

The research is organized by first reviewing the relevant literature and theoretical background about capabilities in cybersecurity and iterative learning. Next, the research methodological approach, including the simulation setup, followed by the evidence of experienced and inexperienced group performance, discussing practical and theoretical contributions, finalizing with limitations and future research directions.

4.2 THEORETICAL BACKGROUND

Given that capabilities in cybersecurity are the core of this simulation, a first brief review presented is based on dynamic capabilities foundations, followed by a discussion of the main theoretical framework based on iterative learning as a premise to avoid delays in developing dynamic capabilities in cybersecurity.

4.2.1 Capabilities in Cybersecurity

To build theoretical foundations in capabilities, we use dynamic capabilities in the IS research field. Seminal definitions of dynamic capabilities underline their nature as an ability (Helfat et al., 2009; Teece et al., 1997; Zahra et al., 2006) and as processes that are identifiable, stable, or characterized as repeatable routines (Eisenhardt & Martin, 2000; Zollo & Winter, 2002). Recently, Steininger et al. (2022) presented the Nomological Net of Dynamic Capabilities for Information Technologies, highlighting a distinction between two levels of outcomes: organizational change, in which dynamic capability results include new or modified ways of operating, and organizational performance, which is a consequence of organizational change created by dynamic capabilities (Steininger et al., 2022). In other words, dynamic capabilities reflect two outcomes in technologies: organizational change and performance.

The IS research field also identifies resources as embracing both capabilities and assets (Piccoli & Ives, 2005), being assets "anything intangible and tangible applied in firms' processes for creating, offering or producing in services or products" (p.109) (Wade & Hulland, 2004), whereas capabilities are "a firm's capacity to deploy (assets)… in combination (with other) organizational processes, to effect a desired end" quoted and adapted by other authors (Amit & Schoemaker, 1993; Steininger et al., 2022; Wade & Hulland, 2004).

Providing a comprehensive, consistent, and pragmatic understanding of the multifaceted construct of dynamic capabilities and following Steininger et al. (2022), we highlighted that dynamic capabilities in the IS research field "encompasses (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 dynamic capabilities to avoid tautologies (Barreto, 2010; Burisch & Wohlgemuth, 2016; Laaksonen & Peltoniemi, 2018; Steininger et al., 2022).

Building upon these perspectives, this experiment brings attention to three CC in the simulation: (1) capacity to scan the environment as 'doing' capabilities (CC_D); (2) acquire, recombine, or eliminate resources (people and technologies) as 'enabling' capabilities (CC_E); and (3) review processes and controls as 'improving' capabilities (CC_I). In other words, CC_D to scan the environment and systems to develop quality solutions for system vulnerabilities; CC_E to support the development of these solutions through people and technology

reconfiguration; and CC_I to perform better processes and controls to predict system vulnerabilities (Al-Matouq et al., 2020; CMMI Institute, 2019).

In CC_D, vulnerabilities in the software development life cycle are crucial and one of the most relevant quality characteristics (Al-Matouq et al., 2020), being inevitable for all kinds of technological projects (Humayun et al., 2022). However, these capabilities vary from project to project because firms tend to consider them 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, CC_D 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 capability is also vital for ensuring the security, safety, and reliability of communications among countless interconnected technologies (Ghobakhloo & Fathi, 2019), considering the nature of buildings, scanning, controlling and reviewing cybersecurity design, solutions and activities.

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

The CC_I encompass 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 the process of experimentality (attempt or experiment with a course of action to acquire a security outcome), manage security across multiple systems and enable 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)

Finally, summarizing the model of these capabilities as dynamic in cybersecurity because they provided change and performance in information security to organizations that are keen on enhancing their cybersecurity posture, we highlight that these capabilities were also identified in cybersecurity practices by Al-Matouq (2020), who validated them in a capability maturity model integration (Al-Matouq et al., 2020). Furthermore, this perspective of dynamic capabilities in information technologies (Steininger et al., 2022) looked at the level of process and abilities that build effectiveness in the management and commitment of firms to implement cybersecurity change to perform efficiently in cybersecurity to reduce vulnerabilities and avoid cyberattacks. This perspective is integrated into the simulation applied in the experiment.

While the growing body of literature on capabilities in cybersecurity discusses the above aspects to a certain extent, the answers about investments in dynamic capabilities development in cybersecurity are not rooted in bringing new forms of maturity levels (Akinsanya et al., 2019) to attend to particular aspects of the complexity in cybersecurity. Therefore, this experiment attempts to capture how uncertainty surrounding cyber-risks and delays in developing dynamic capabilities affect the potential performance scenario of firms in profit losses because of cyber incidents (Jalali et al., 2019).

4.2.2 Capabilities in systems vulnerabilities and uncertainty

The nature of uncertainty caused by cybersecurity threats combined with frequent technological change and unpredict vulnerabilities has caused remarkable anxiety and doubts in which capabilities have to expend time and money to be well prepared against cyber threats (Fagade et al., 2017; Jalali et al., 2019). For example, small and middle enterprises do not experience cybersecurity as much as larger firms usually do, and therefore, they offer little attention to investing in cybersecurity capability development. They usually create enormous gaps in cyber-risk awareness and the real state of system vulnerabilities (Madnick et al., 2017). As a consequence, an underestimation of potential vulnerabilities occurs, and they usually take time to become active in detecting and responding to cyber incidents or even start working preventively.

The challenges faced by firms associated with cybersecurity requirements are potentially impacted by the development of appropriate capabilities to cope with cyber risks and technological evolution. The lack of knowledge and awareness about virtual environment

threats lead firms to make incorrect decisions about where to invest and what to do about it. Furthermore, cybersecurity remains an incognita even for those who are familiar with the subject. Some authors (Shaikh & Siponen, 2023) stress the need for firms to analyze aspects of their cybersecurity performance and use them as "feedback for investment decisions, making these decisions data-driven and based on firm-specific needs" (p.1). Therefore, it is important to address this issue among experienced and inexperienced individuals because of their potential contribution to decision-making processes inside firms on this topic.

Broadly, according to Chatterjee and Thekdi (2020), research on cyber vulnerability involves the prediction and identification of dynamic cyber threats, and managing risk for these cyber-enabled systems also poses various preventive, reactive, and proactive cybersecurity challenges (Chatterjee & Thekdi, 2020). In this vein, different capabilities may act as preventive resources, such as scanning virtual environments (CC_D); reactive resources, such as acquiring, eliminating, or reconfiguring people and other technologies (CC_E); and proactive resources, such as standardizing processes and controls to enhance cyber protection (CC_I) (Al-Matouq et al., 2020; CMMI Institute, 2019). These capabilities may reduce the level of system vulnerabilities in a cyber ecosystem.

Different sociotechnical aspects may affect the decision process about resource allocation to create a cybersecurity posture inside firms. As highlighted by Fagade et al. (2017), "optimal resource allocation to information security is often affected by intrinsically uncertain variables, leading to disparities in resource allocation decisions". Additionally, predictable and unpredictable aspects of cybersecurity are not a mere matter of guesswork but rather organized and synchronized capabilities against an unorthodox way of thinking (Steinmetz, 2015). Hence, firms that insist on a reactive posture against investment in developing CC may cause profit losses in the cost of cybersecurity breaches in the future (Master et al., 2022). However, some authors (F. Xu et al., 2019) highlighted that reactive investments for cybersecurity improvement earn positive abnormal returns.

The reactive posture is quite common and only becomes critical after detecting a concrete cyber-attack where a firm´s computer-based systems may no longer be properly recovered or still remain vulnerable. Thus, providing a fictitious virtual environment to enhance awareness in understanding systems vulnerabilities and the needed capabilities to reduce potential losses may offer experienced and inexperienced individuals a learning process to become familiar with uncertainties and cyberthreats (Disparte & Furlow, 2017; Jalali et al.,

2019). In this vein, potential opportunities to learn about developing, investing, and understanding CC may foster a new mindset in practitioners.

4.2.3 Experience and inexperience in cybersecurity

The areas of capabilities in cybersecurity generate different perceptions of importance between experienced and inexperienced individuals. For example, some authors (Catal et al., 2023) argued that cyber-physical systems, vulnerabilities, and software life cycles are the areas of capabilities with the greatest difference in this perception of importance. In other words, experienced and inexperienced individuals differ in their understanding of this importance. In cybersecurity, some authors identify that there is a difference in the rational of decision-making between experienced and inexperienced individuals, and the level of self-reported experience established in the literature is diversified (Catal et al., 2023; Jalali et al., 2019; McClain et al., 2015). It is also found in the literature that self-reported experienced individuals exhibited less secure behaviors than self-reported inexperienced individuals (Cain et al., 2018).

Moreover, the literature also points out experience as individuals self-reported with high familiarity with the term cybersecurity – either through social media, internet conversations and traditional media, virtual classes at the university, IT or scientific journals, or personal experience with cyber-attacks. On the other hand, inexperience such as individuals self-reported no awareness, knowledge, or personal experience with information security issues (Zwilling et al., 2022). Nevertheless, other perspectives about experience in cybersecurity presented by different authors are also successes, failures, business challenges when an individual responds to information security and cyber risks, or the effectiveness of hands-on experience being used in virtual environments to effectively handle cybersecurity incidents (Beuran et al., 2023; Daniel et al., 2022; Zacharis & Patsakis, 2023). Furthermore, the literature also noted that experience is expressed by a continuous capacity to identify anomalous network activity in a high-noise environment and judge whether to pass this information up to a superior to investigate further (Van Der Kleij et al., 2022).

Therefore, considering the complexity of defining experience and inexperience in cybersecurity because of multiple operators, tools, and locations where cyber incidents may occur and be classified by individuals with different levels of experience and judgment (Van Der Kleij et al., 2022), we follow Zwilling et al. (2022), who define experienced individuals as those self-reported with high familiarity with the term cybersecurity and a personal experience

with cyberdefense. Inexperience is defined as individuals self-reported with no awareness, no knowledge, and no personal contact with cybersecurity issues (Zwilling et al., 2022).

Additionally, for the purpose of this experiment, experience levels are reported in years following some authors in the literature (Jalali, 2014; Jalali et al., 2019). On the other hand, when an individual self-reports an inexperience in cybersecurity, the evidence in years is identified as zero. However, regardless of experience levels, this simulation can shed light on the impact of cybersecurity to encourage inexperienced and experienced individuals to behave more securely when confronted with cyber security incidents (Fisher et al., 2003; Zwilling et al., 2022). Thus, we hypothesized the following:

H1 – Investments between experienced and inexperienced groups in cybersecurity capability development differ because of sociotechnical characteristics, and

H2 – Investing in cybersecurity capability development can be learned iteratively.

In this vein, this experiment simulates an environment of cyberattacks to investigate the learning process of participants in proactive and reactive postures to invest in cybersecurity capability development. We present how the simulation addresses the uncertainties in a cybersecurity ecosystem in the next section more clearly.

4.3 METHODOLOGICAL APPROACH: SIMULATION MODEL STRUCTURE AND FORMULATION

This simulation demonstrates how experienced and inexperienced groups perform through investments in developing CC . It also investigates whether this process can be learned iteratively. Making use of the experimental method to facilitate the analysis in a simulation environment (Sterman, 2001), we analyze the proactive and reactive posture of investments in cybersecurity capability development through dynamic system modeling, which is not a new approach in the IS research field (Hwang & Helser, 2022; Jalali et al., 2016; Meland et al., 2019), especially in relation to business capabilities (Jalali et al., 2019). The simulation experiment will examine this issue from a systematic and multidimensional perspective to identify the impact of investments in capabilities as resource allocation from a portion of profitability.

Methodologically, we follow four stages suggested by OliveiraJr et al. (2020) for experiments: (a) planning, allowing more control of the experiment by previously defining, for example, objective, hypotheses, instruments, and variables; (b) operation, with a preoperational stage in a pilot test, which executes the experiment according to its plan, mainly by collecting

data with instruments or designed systems; (c) analysis based on observed data (samples), such as statistics and tests of normality and hypotheses; and (d) dissemination, responsible for disclosing the planning, operation, analysis and interpretation of the experiment to the interested public, such as researchers and professionals in the sector (OliveiraJr et al., 2020). Table 15. Experiment phases description describes the different stages followed during the experiment following the guidelines of OliveiraJr et al. (2020), who proposed the "Experimentation in Digital Forensics Conceptual Model (ExperDF-CM)". Each step of the experiment is developed to explicitly consider the correctness of the research design, its operationalization, its description, and its dissemination. The advantage of this framework is that it makes everything explicit and can thus act as a trigger for debate (Mingers & Standing, 2020). Such considerations will clearly lead to the possibility of other studies.

Table 15. Experiment phases description

Planning	Hypothesis	H1 – Investments between the experienced and inexperienced groups in CC es development differs because of sociotechnical characteristics. H2 – Investing in dynamic capabilities development in cyber protection can be learnt iteratively.
	Experimental Unit	Simulator
	Analysis	Profit accumulation performance and learning process by participants
	Validation	The simulator will be developed by technology experts under the supervision of the researcher based on a system dynamics simulation model (Jalali et al., 2019; Khalid Khan et al., 2022). The model will include three main dimensions: CC, computer-based information systems and cyber incidents.
	Type of Experiment	Independent Replication in which one or more design elements vary from the original experiment applied in Jalali et al. (2019).
	Sample	Non-Probabilistic, where participants do not have the same chances of being selected. Furthermore, we followed Kelley's et al. (2017) approach who applied general guidelines for choosing an appropriate sample size and ensure sufficient power effect sizes when using a multivariate approach to analyze repeated measures data. Three factors were used to define the sample size: the desired predictive power, the size of the anticipated effect and the correlation between scores at each level. To reach a predictive power of 0.95 with $\alpha = 0.05$ (standard for social science) for an effect size between 0.50 and 0.75 for two levels (which is this case) a sample between 48 and 105 participants is acceptable. The final sample was 119 participants.
Pre-Operation	Setup	Algorithm was developed based on a "system overview" ecosystem and capabilities investments
	Training	An instructional model was built for participants and validate by three experts in information security.
	Pilot Project	A pilot test was carried out with experts before the launch of the experiment
Operation	Procedures	Groups played the simulation in the same room at the same time. To avoid social influences, they will not reveal their results at any time. Necessary background information was provided before starting the experiment watching an example run. Before starting, participants perform practical simulation in test mode to clarify any doubts. Simulation level one takes five minutes, then play level two for another five minutes. Participants is informed of the difference between the two levels only at the end

		of the simulation. Appendix F shows details about the processes that involved the operationalization of the experiment.
	Data	Original data is generated after the end of the experiment through a excel file
	Material	Computers available in the experimental rooms used to conduct the simulation were the main material resource of accessing the simulator located at online platform https://en.cybermuli.com/#/
	Participants	Participants were split into two groups: the experienced group (experimental) and the inexperienced group (control). The experimental group will include academic students with cybersecurity experience. The control group will include academic students enrolled in business administration course and none of whom had any previous experienced in IT or cybersecurity.
	Instrument	See Figure 1
Analysis and Interpretation	Analytical Technic	Quantitative approach (normality test, t test, mean, standard deviation, variation index), circular statistics (testing whether phenological patterns differ between or among individuals, species, or entire communities by comparing angles, mean angles, or mean vectors) (Morellato et al., 2010) and variation of performance in leaning iteratively (linear slopes).
	Data Plot	Tables, Circular Charts, Plot charts, and Linear charts.
	Limitations	Similar applications have been developed in other fields such as climate policy (Sterman et al., 2015), strategic management (M. M. Yang et al., 2016) and health policy (McFarland et al., 2016), cybersecurity (Jalali et al., 2019), however, the general advice for simulators is to keep the model as simple as possible to meet the objectives (S. Robinson, 2008).
	Validation	To internal validity, we allow open questions from participants to support their planning and conducting the simulations runs. To mitigate external validity, we provided participants information containing several data about how to use the simulator in training sections before the simulations. Even though we could not generalize the findings, it was possible to demonstrate evidence on the feasibility of the learning process. Conclusion validity was treated by inviting experts who worked on the projects to make the attributes of simulator closer of reality.
Reports	Dissemination	A trusted repository on Harvard Dataverse (Pigola, 2023) is used for storing the data through reports, data set of information gather, simulator registration on INPI (Instituto Nacional de Propriedade Intelectual), experiment activities; and documentation of experimental problems.

Note. Elaborated by author (2023)
Source. OliveiraJr et al. (2020)

Figure 4 shows the simulation model structure. The simulation model is relevant to the game because based on the ecosystem of computerized security systems, the participant makes the decision to invest (a percentage of profit) in cybersecurity capability (CC) development in three dimensions: doing capabilities (CC_D), to scan virtual environments to avoid that "nonrisk system" (SNR) jump to "systems at risk" (SR) because the absence of CC_D is a risk promotion to SR; improving capabilities (CC_I) to standardize process and controls, to intensify the detection process of SR and "systems affected" (SA); and enabling capabilities (CC_E), to acquire, eliminate or reconfigure people and technologies to support activities of patching

"systems affected and detected" (SAD) or keep SNR in place. Each security system category is impacted by an output of development (I). The advance of investments in CC is calculated as

$$\frac{CC_{(t)}}{d_{(t)}} = I_{(t)}$$

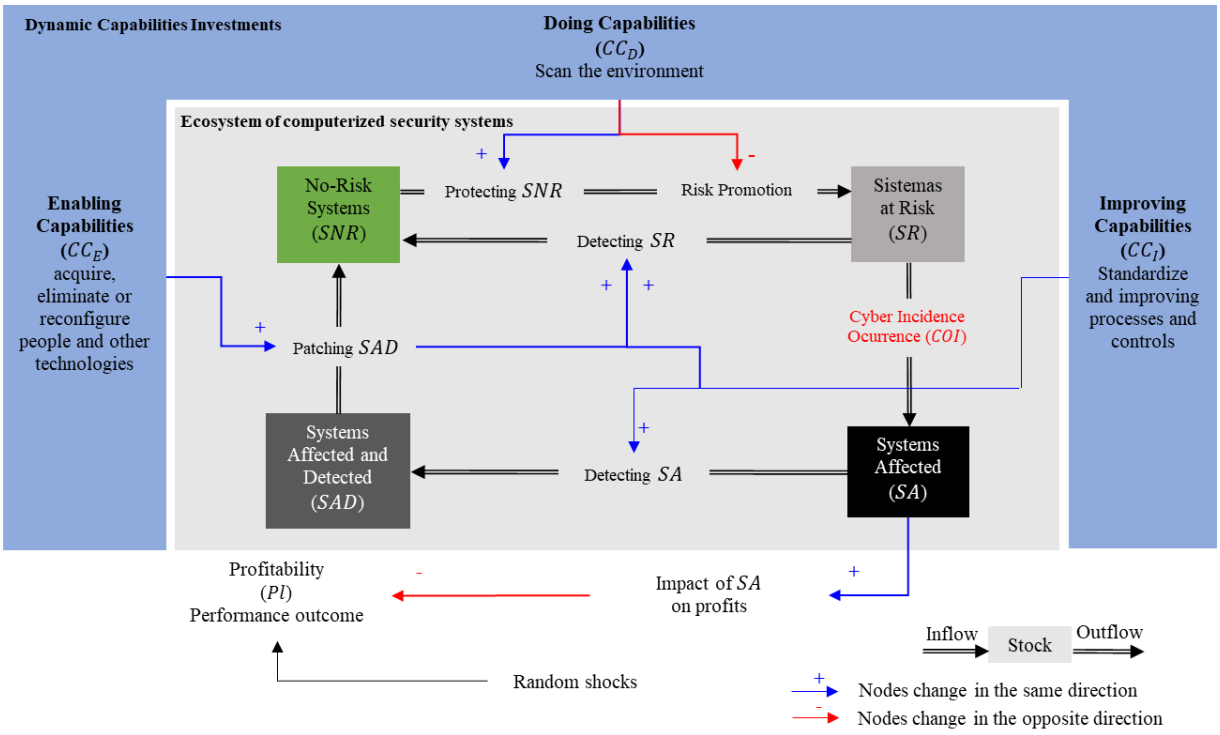
where,

CC is total of investments in CC_D, CC_I andCC_E;

d is the month of reference where the investment is made, and;

t is the time of simulation defined in six months in level one and three months in level two. Similar formulations were used in other settings (Jalali et al., 2019; Rahmandad, 2012; Rahmandad & Weiss, 2009).

Figure 4. The general structure of the simulation model



Source: Elaborated by author (2023)

The simulator assumes multiple computerized security systems overview in the fictitious scenario of an organization. They are initially in the SNR. Considering a low level of investments in capabilities, the simulator moves SNR to SR, and how quickly this happens is considered risk promotion due to the absence of investments in CC_D. Cybersecurity is one of the most relevant software quality characteristics and is inevitable for all kinds of security systems projects, although it varies from project to project because firms tend to consider it as

an afterthought. Therefore, when bugs and defects are discovered early in the production process, they are easier and less expensive to fix than those discovered later (Al-Matouq et al., 2020; Humayun et al., 2022). Thus, the lower the investment in CC_D is, the greater the risk promotion. CC_D help to identify cyber threats and limit SR size to move back to SNR. The out and inflow from SNR to SR is determined as

$$SR_{(d)} = SNR_{(d)} \cdot \left(1 - \frac{\frac{1}{CC_{D_{(d)}} + 1}}{I_{(t)}}\right)$$

where, $I_{(t)}$ is always assumed to be six months in level one and three months in level two. SR are defenseless, potentially being affected early in a cyber-attack. Once affected by a cyber occurrence incident" (COI), the simulator changes the systems SR to SA. While it is acknowledged that the risk of occurrence incidents is significant in reality (Fernandez De Arroyabe et al., 2023; J. Wang et al., 2015; Willison & Warkentin, 2013), we follow Jalali et al. (2019), who pointed out that simplifications do not impact the relevance of simulator game results since most successful cyber incidents result in profit and data loss or operational disruptions regardless of their nature (Jalali et al., 2019). The COI rate is measured as

$$COI_{(t)} = SR_{(t)} \cdot CI_{(t)}$$

where, $CI_{(t)}$ is an exogenous portion meaning cyber incidents throughout the simulation. COI impact SR moving systems to SA that have the potential to reduce the profitability (Pl) of the fictitious organization. Cyber incidents often take time to be detected (Sangari et al., 2023), therefore SR tend to become SA easily. Additionally, to build a higher CC maturity level is initially necessary a higher incident probability (Dinkova et al., 2023) to build a learning process. Therefore, the out- and inflow from SR to SA is determined as

$$SA_{(d)} = COI_{(t)} \cdot \left(1 - \frac{\frac{1}{CC_{D_{(d)}} + CC_{I_{(d)}} + 1}}{I_{(t)}}\right)$$

Notwithstanding, the simulation allow participants detect SA and invest more in CC_I to achieve additional outcome in the systems overview moving SA to SAD at a rate of

$$SAD_{(d)} = SA_{(d)} \cdot \left(1 - \frac{\frac{1}{CC_{I_{(d)}} + 1}}{I_{(t)}} \right)$$

SAD may change the status in the presence of CC_E and CC_I investments to move systems to SNR. If there is a proper investment in these capabilities, SAD may be recouped to SNR. In practice, the decision to commit to CC investment results in immediate costs associated with the adoption of new technologies, people and processes, including learning and switching costs (Acquisti & Grossklags, 2003; Bowen et al., 2011; Jalali et al., 2019). The correction rate at this point is defined by

$$SNR_{(d)} = SAD_{(d)} \cdot \left(1 - \frac{\frac{1}{CC_{E_{(d)}} + CC_{I_{(d)}} + 1}}{I_{(t)}} \right)$$

Additionally, systems may not be directly at risk due to proper investments in CC_D, CC_I and CC_E to protect SNR from cyber-attacks in advance and hence slow the flow of systems to SR. The inflow of SNR is determined as

$$SNR_{(d)} = SR_{(d)} \cdot \left(1 - \frac{\frac{1}{CC_{D_{(d)}} + CC_{E_{(d)}} + CC_{I_{(d)}} + 1}}{I_{(t)}} \right)$$

The multiple computerized security systems overview helps to streamline and communicate the goal during the experiment, and it also supports better monitoring of the iterative decisions. SA and I impact profit losses (Pl). In general, cybersecurity incidents are manifested in two forms: cash flow losses and reputation damage (Crossler et al., 2013; Jalali & Kaiser, 2018; Kalderemidis et al., 2022). This means that the output of development from investments made in each capability when applied incorrectly based on systems overview

increases Pl. Additionally, unbalanced investments may increase the number of SA, also impacting profitability. Pl follows a nonlinear functional,

$$Pl_{(d)} = -1 . \left(\frac{SA_{(d)}}{I_{(t)}}\right)^{\frac{1}{2}} . \left(\frac{1}{CC_{(d)}}\right) . \left(1 + I_{(t)}\right)^{\frac{1}{100}}$$

However, when the participant is aware of computerized security systems overview and invests in the CC accordingly, the impact will be on profit earnings (Pe), which follows a nonlinear functional

$$Pe_{(t)} = T . RP_{(t)} . \left[1 + \left(I_{(t)} . \frac{1}{10}\right)\right] - \left(CC_{(d)} . PA_{d_{(t)}}\right)$$

where

T is the total number of existing systems, which is equal to 100

RP is the percentage of profits invested in CC

PA is the profit accumulated at $d_{(t)}$

Participants can monitor earnings and losses over time and adjust their decisions based on the computerized security systems overview receiving notice about profits, earnings or losses related to the decision of investment parameters. The trade-offs between the two main effects of CC investments are profiting reduction when investments are not receiving adequate treatment and the ability to protect the organization from costly cyberattacks. In other words, investing in CC development means reducing the impact on profit losses. Therefore, investing in these capabilities (CC_D, CC_I and CC_E) potentially helps to reduce cybersecurity impacts.

This means that the level of risk is reduced considerably, avoiding profit losses, when investments in CC are balanced and learned by the participants. The goal is not losing and earning profits to compensate for the investment (specifically those accrued over the simulation course) by allocating investments in CC more efficiently. Each simulation run will span 60 months. The trade-off between profit and protection implies a challenge increasing the complexity of the decision-making process because of the uncertainties in cyber-attacks. Finally, the participants decided which type of capabilities to invest to reduce the risks inherent in the systems ecosystem of the fictitious firms, balancing the profit accumulated. The

simulation begins with $1,0 million in profit accumulated and 100 computerized systems in the ecosystem (system overview).

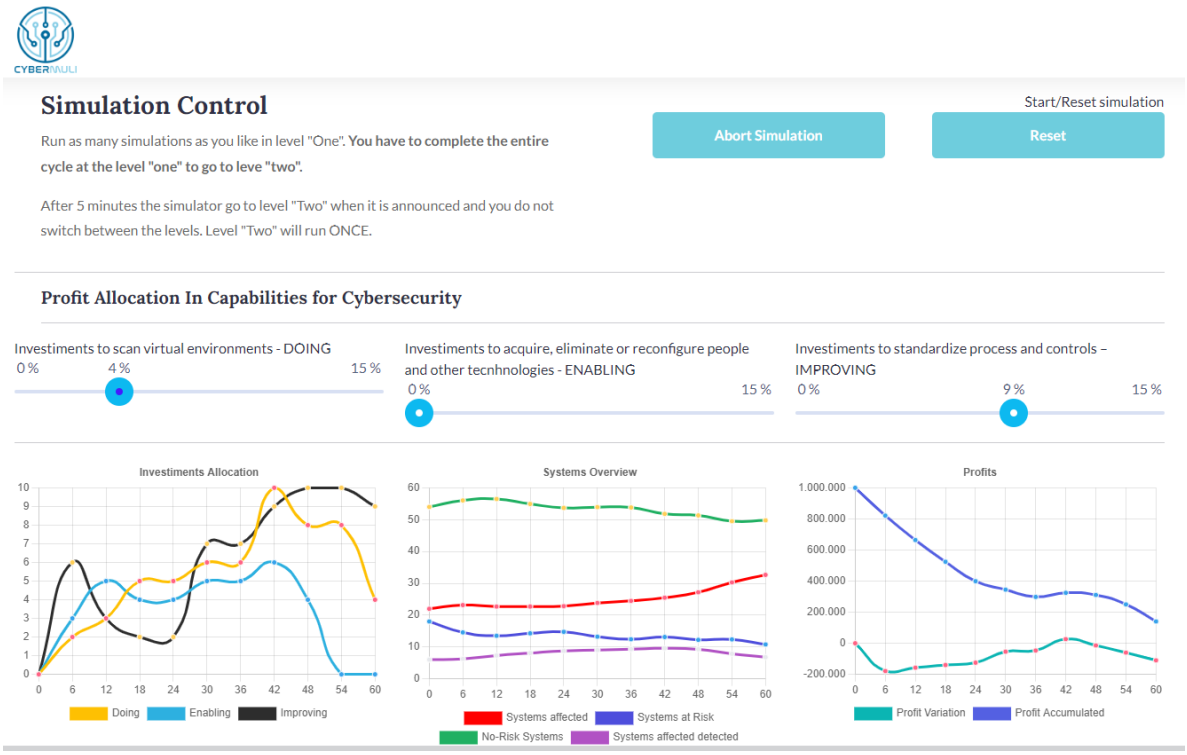
Aleatory COI with different levels of impact occur during each of the two levels of the simulation within ten minutes each (the greater the impact of the attack is, the greater the influence on profit reduction). It will evaluate the differences in decision-making according to the scenarios over time. To keep the simulator simple, all attacks are determined as external attacks coming outside the firm's network not categorized by type. At level one (deterministic), the cyber incidents are fixed in time and impact, and at level two (nondeterministic), they happen randomly in time and impact following a nonuniform probability distribution. With the profit result differences between the two levels, we expect an iterative learning of how to maximize profit after several rounds of investing in dynamic capability development by repeating the simulations on the optimal combination of investment parameters.

Figure 5 shows a screenshot of the online simulation.

Simulator modeling is simplified because complex systems in a detailed and complicated model do not always translate into a more realistic simulation (Sull & Eisenhardt, 2015). The simplicity of our model helps us to better explain decision-making behavior based on resource allocation dynamics. It also allows participants to better engage with the model, relating it to their own organizations' evolution in cybersecurity.

Participants were physically tested in different locations. Data gathering occurred in two different universities in three distinctive locations and five groups in May and June 2023. Against social influences (Jalali, 2014), participants were not allowed to discuss or reveal their results at any time during the simulation. A necessary background was provided in a short presentation of the simulator and in the simulation introduction already in place inside the simulator. They were informed that the purpose of the simulation was to maximize profitability in a fictitious company after sixty months and that no investment in CC was already in place at the beginning of the simulation. In step one, participants had an opportunity to run the simulation many times as a practice mode and raise questions about doubts about the simulator. Participants were not aware of the difference between the two levels until the results were presented at the end of the experiment.

Figure 5. Screenshot of the online simulation



4.4 EVIDENCE OF EXPERIENCED AND INEXPERIENCED GROUP PERFORMANCE IN THE SIMULATION

The data from the CC (CC_D, CC_I *and* CC_E) were collected in each individual simulation as well as information related to profit accumulation over the 60 months in each run (levels one and two). The final profit accumulation in each full simulation measured the individual performance of each participant. Incomplete simulations (when the player left the simulation before reaching the last month) were not included in the analysis. Table 2 shows the data summary of the participants, and the simulation runs. In the next sections, two individual runs are presented (reactive and proactive runs) followed by a comparison between the outcomes between experienced and inexperienced groups, and we highlight key findings that answered the research questions.

Table 16. Simulation Data Summary

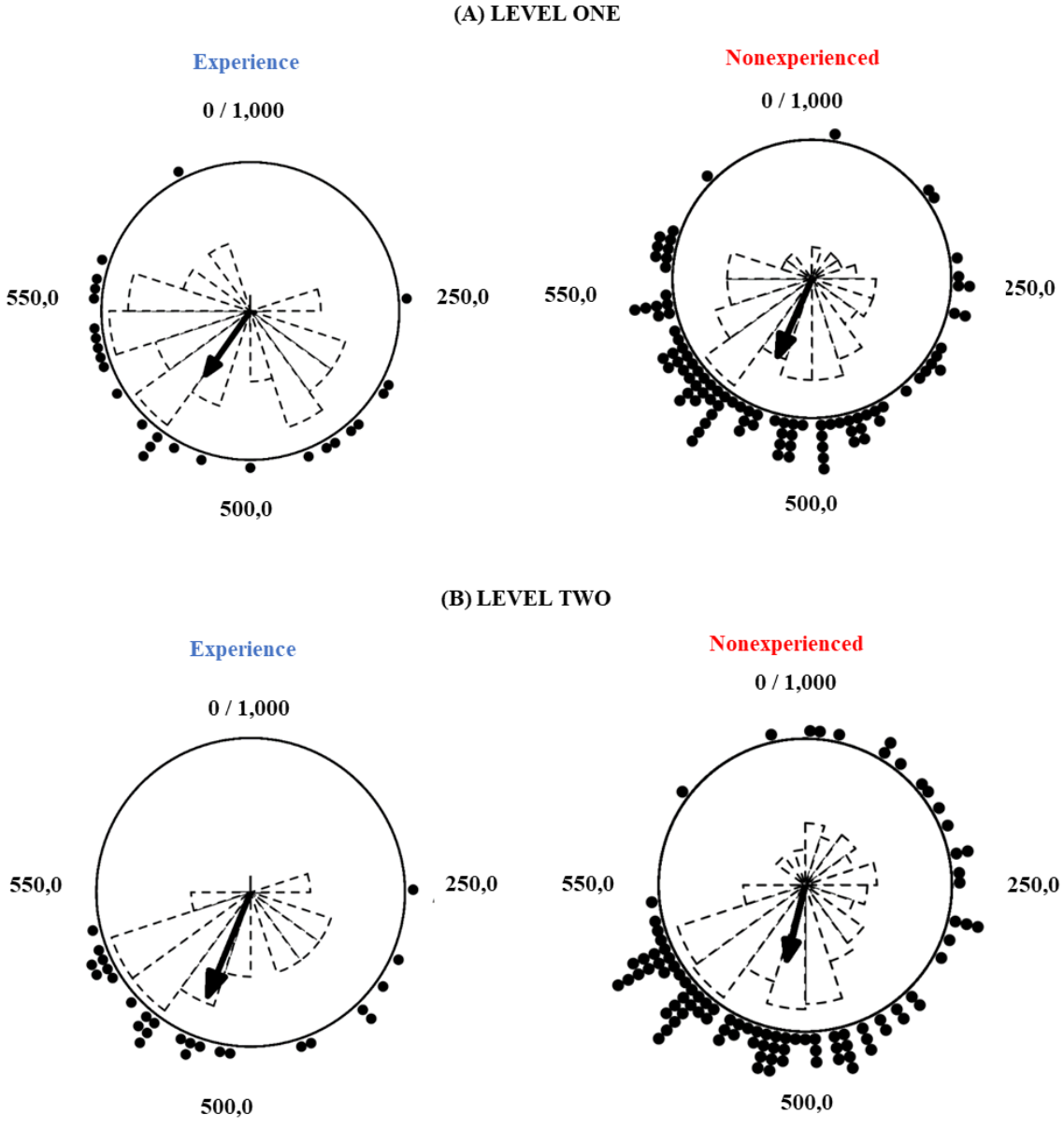
Groups	Number of Participants	Average of experienced in cybersecurity	Individual Simulation Runs		Average per participants (simulation runs)	
			Level One	Level Two	Level One	Level Two
Experienced	26	4 years	286	546	11	21
Inexperienced	93	-	1023	1953	11	21

Note. N = 119.

Figure 6 presents the circular statistics of individual participants' best performance for each level. Both groups displayed large variations in profit accumulated in the two levels; however, the average performance in level two was less than that in level one, indicating that aleatory cyber incidents inherent in level two reduced the capacity of participants to apply the right capabilities when necessary. Furthermore, in level one, the pattern of cyber incidents is fixed to offer an optimal set of stable conditions for the three parameters of capabilities (CC_D, CC_I and CC_E) to mitigate profit losses. In level one (Figure 6-a), the experienced and inexperienced groups presented similar performance, but in level two (Figure 6-b), the inexperienced group presented more variability in the distribution of accumulated profits. The profit accumulated skewed to poor performances when compared to the experienced group (average of M$250). This result confirms hypothesis 1 that investments between the experienced and inexperienced groups in cybersecurity capability development differ because of sociotechnical characteristics.

However, analyzing whether the experienced group had better general performance than the inexperienced group because we were expecting more proactive investments from the experienced group, the t test reveals that no significant difference exists at $\alpha = 0.05$ (Table 17). This means that collectively, the experienced group does not make better decisions to develop cybersecurity capacities than inexperienced participants. These results corroborated the findings of Jalali et al. (2019), who highlighted that "experienced players do not make better decisions to develop CC than inexperienced players" (Jalali et al., 2019). Considering the high variation in performance results, we next evaluated the effect of iterative learning to answer the main research question.

Figure 6. Distribution of participants' performance in the levels



Level One	Mean	S.D.	Var.	**Level Two**	Mean	SD	Var.
Experience	547,57	1.138	0.477	Experience	473,26	0.799	0.274
Nonexperienced	525,17	1.003	0.395	Nonexperienced	407,54	1.138	0.477

Note. all values are calculated on a normalized period of 2π. (→) indicate mean vector

Table 17. Paired sample statistics

Experienced versus Inexperienced	t	W
Level One	-1.107	0.921*
Level Two	-0.386	0.875*

Note. Student's t test (t) not significant at α = 0.05; Test of Normality Shapiro–Wilk (W) suggested a deviation from normality at $p < 0.05$ (*)

4.4.1 Iterative learning of experienced and inexperienced groups

Comparing the individual performance of participants to understand the effect of the iterative learning process at level one and at level two, we began by identifying the top performances of each group in each level. In the experienced group, we identified 8 participants who reached a positive profit accumulated at the end of level two compared with the end of level one (after running 60 months), representing 30.8 percent of the total population. In the inexperienced group, we identified 29 participants in the same situation, representing 31.2 percent of the total population. This means that the level of people who achieve an effective learning process is similar in both groups. Appendix G also shows the average of investments made by participants in each capability at both levels. These findings corroborate Melane et al. (2019), who emphasized that students inexperienced in security modeling perform similarly to security experts in a well-defined scope and familiar target system/situation. The authors showed that inexperienced people tend to focus on preventive barriers, and experienced people balance this with incident management and reactive barriers (Meland et al., 2019).

Correlation analysis was also used to analyze the effect of iterative learning, i.e., the effect of running a sequence of simulations to enhance performance. Table 18 highlights the correlations between simulation runs and profit accumulated in each run. Negative correlations with significant p values (<0.001) are observed in both levels and groups. These findings show that experienced and inexperienced groups did not have relevant improvements by conducting more simulation runs. As mentioned earlier, a better performance between the levels can only be reached by making an appropriate connection between the three capabilities and the systems overview. Participants needed to understand which capabilities are needed to develop incident response management in the simulator (Bitzer et al., 2023). Proactive decisions on investing in capability development in cybersecurity are directly associated with the right capabilities with the type of system conditions. In other words, CC_D (scan virtual environments) are effective when systems are at risk of detecting potential threats, CC_E (eliminating or reconfiguring technologies and professionals) are efficient when affected systems need attention to actions of eliminating virus or any other threats, and CC_I (standardize processes and controls in information security) are relevant when systems affected and already detected improve the cybersecurity posture about risks and robust processes and controls.

Table 18. Correlation between simulation runs and profit accumulation

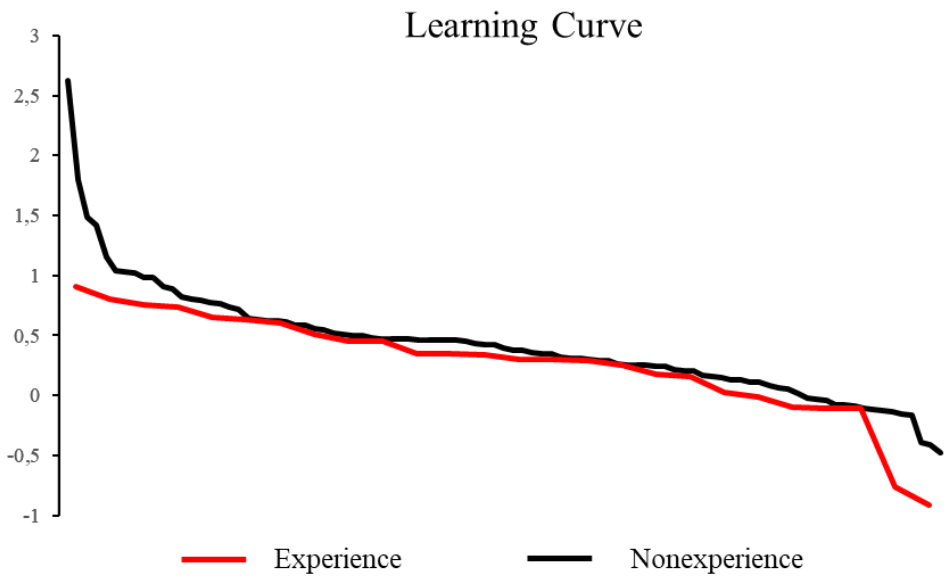
	Level One	Level Two
Experienced	-0.420	-0.159
Inexperienced	-0.591	-0.142

Note. * $p < 0.001$

Additionally, the variation in participants' performance (profit accumulated) through the sequence of simulation runs (the number of runs of each participant) at each level permitted us to sort the linear slope of the participants in descending order to show the greatest improvement in profit accumulation over the course of the simulation runs. In

Figure 7, we present the linear slope curve of each participant, which means the participant's improvement performance over all simulation runs between the levels. The participants were sorted by their ranks between level one and level two. In the experienced group, 71.4 percent of the participants presented a positive linear slope against 83.9 percent in the inexperienced group. This means that the inexperienced groups presented a higher iterative learning process than the experienced group. According to Jalili et al. (2019), "considering the linear slope of a player's performances allows us to observe all of their run data and observe their learning process" (Jalali et al., 2019). These results corroborate Karagiannis and Magkos (2021), who also emphasized positive outcomes in terms of technical skills and knowledge acquisition through simulations where students felt more confident about their skills and were highly engaged in the learning process (Karagiannis & Magkos, 2021).

Figure 7. Learning curves of individuals – Linear Slope



Source: Elaborate by author (2023)

The participants in the inexperienced group had a slightly higher performance slope than the experienced group, which means that the best participants in level one learned the principles of the simulations between capabilities and the systems conditions to establish their strategies of investments in CC in level two. This finding corroborates (Shreeve et al., 2023), who emphasized that individuals with little cyber security expertise are able to use logic and traditional risk management thinking to make cyber security. However, even though some of them had this perception, they were surprised in level two because of the random cyber incidents, and therefore, they performed poorly. For example, in the experienced group, the top ten participants had an average decrease of 42 percent from level one to level two. In the inexperienced group, the average was 75 percent of the decrease ranking. This means that the classification of participants seems to change more arbitrarily (Jalali et al., 2019). These findings corroborate Hwang and Helser (2022), who highlighted that "users characteristics including gender, age, computer experienced, knowledge and perception, are attributes that can impact users' susceptibility to cybercrimes and hence learning outcomes" (Hwang & Helser, 2022). These findings also confirm hypothesis 2 that investing in capability development for cyber protection can be learned iteratively.

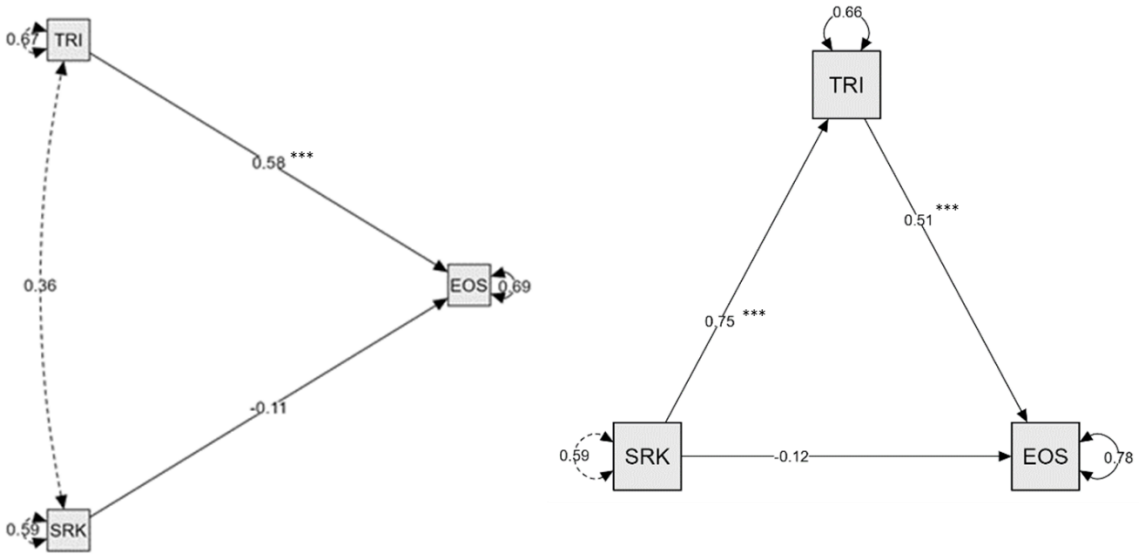
4.4.2 Trust and Knowledge impact in the simulation

Simulations in cybersecurity have been developed to support both individuals and firms in sharing awareness of cyber threats. However, their effectiveness has been questioned (Hwang & Helser, 2021), although some authors (Ekelund & Iskoujina, 2019) have emphasized that optimal security investment levels can be found through computer simulation, and Sewak et al. (2022) highlighted that "different techniques and algorithms have shown great promise in learning applications ranging from games to industrial processes. These algorithms have recently also been used in cybersecurity, especially in threat detection and protection, where these are showing state-of-the-art results" (Sewak et al., 2022).

Therefore, we analyzed the perception of participants at the end of the simulation to understand the effectiveness of the experiment based on participants' perception. We surveyed their trust and knowledge perceptions after the experiment to identify how they perceived the experience of learning. This analysis is a result of a survey instrument applied after simulation conclusion, and it is not part of the general structure of the simulation model presented in Figure 4. The instrument adopted came from previous research (Aleroud et al., 2020) and included

four items measuring security-related knowledge (SRK), four items measuring trust-related issues (TRI), and the effectiveness of the simulator (EOS). We used a 5-point Likert scale, where 1 indicates total disagreement and 5 indicates total agreement. Based on this scale, we follow Aleroud et al. (2020), where a mean value of responses between 1 and 2.33 was considered low, a mean value between 2.33 and 3.66 was considered moderate, and a mean value between 3.66 and 5 was considered high (Aleroud et al., 2020). In structured equation modeling, the variables SRK and TRI are latent formative variables that are calculated by the mean of all indicators. All statistics were calculated using JASP 16.4 software; Appendix H shows the survey instrument factor loadings and statistics related to the data. Figure 8 shows the final measurement models. Table 19 highlights the effect parameter estimates among the variables under mediation analysis.

Figure 8. The final measurement models of trust and knowledge in the simulation



Note. * p <.001; ** p < 0.10

Table 19. Analysis of estimation effects of trust and knowledge

						95% Confidence Interval	
Mediation		Estimate	Std. Error	z value	pvalue	Lower	Upper
Direct	SRK → EOS	-0.119	0.129	-0.917	0.359	-0.378	0.111
Indirect	SRK → TRI → EOS	0.382	0.090	4.263	< .001	0.181	0.669
Total	SRK → EOS	0.264	0.117	2.261	0.024	-0.010	0.546

Note. Delta method standard errors, bias-corrected percentile 5,000 bootstrap confidence intervals, maximum likelihood estimator.

The findings revealed that security-related knowledge (SRK) positively affects trust-related issues (TRI) (β = 0.751; p <.001) in the experiment, but it does not positively and significantly influence the effectiveness of the simulator (EOS) (β = -.119; p = 0.359). On the other hand, trust-related issues (TRI) significantly influence the effectiveness of the simulator

(EOS) (β = 0.509; p <.001), enhancing the total effect of SRK on EOS about the simulator (β =.264, p < 0.024). This means that SRK, when mediated by TRI, exerts more influence on EOS. These results corroborate those of other authors who highlighted that trust can significantly predict both subjective and objective security behavior (Workman, 2008). Another explanation for the significant effect of trust in our study can be cultural factors (Zhang et al., 2012). Cultural differences were found to have effects on trust, where collectivistic cultures tend to trust more than individualistic cultures (Yamagishi & Yamagishi, 1994). The effectiveness of the simulator was evaluated by participants as relevant to the practice of learning in investing in cybersecurity capability development. This information is relevant to confirm that this experiment supports experienced and inexperienced people to learn about CC.

4.5 DISCUSSION ABOUT THE IMPLICATIONS OF THE EXPERIMENT

It is important for firms to understand the impact of CC through iterative learning to produce educational initiatives among employees and how proactive investment decisions impact the dynamics of risks and costs that potentially affect profitability in the case of cyber-attack. For example, an attacker's breach efforts are proportional to the economic benefit to be gathered, irrespective of the nature of the attack (Gupta et al., 2021); therefore, any cyber incident is costly. Additionally, firms may use these results to introduce a different approach to open-source cybersecurity training platforms (Beuran et al., 2023) or standard training sections of employees (Jalali et al., 2019) scaping from traditional e-learnings. As mentioned by Sharma et al. (2020), "users with similar instances of cybersecurity attacks can increase their risk-averse behavior" (Sharma et al., 2021).

Optimum decisions in cybersecurity are utopic. However, repetition and learning may bring decision-makers appropriate conditions to gather accurate information to the best approach in resource allocation in cyber defense. Furthermore, this experiment highlighted how crucial it is time and action to invest in capability development because threats in information security do not say when, why, where or how they will happen. Finally, the cybersecurity community in countries with more individualistic cultures has recently made more efforts to intervene in cyber awareness than those with more collective cultures. Examples include establishing capability maturity models for incident response (Bitzer et al., 2023; CMMI Institute, 2019) or top management commitment to capability implementation and assimilation in information security (Barton et al., 2016; Bulgurcu et al., 2010; C. Hsu et al., 2012; Pentland et al., 2017). Therefore, cybersecurity is not a matter of "if" a firm will be affected, but it is

currently a matter of "when" and "at what level" (D'Arcy et al., 2020; Jalali et al., 2019; Kour & Karim, 2020).

This experiment provides a proactive reaction to invest in CC development, enhancing awareness that these investments are not related to a mere return on investments but a prediction of profitability losses. Moreover, experienced individuals may not be a predictor of cybersecurity events because in practice, they may not work accurately. The effectiveness of iterative learning is a reality even if the results are unexpected. Finally, the role of trust facilitates the process of learning iteratively regardless of the knowledge in cybersecurity.

4.5.1 Theoretical Implications

Although dynamic capabilities have been extensively applied in the IS research field, there has been no comprehensive evaluation of them from a useful theoretical perspective. However, the approach that dynamic capabilities encompass abilities is acceptable (Steininger et al., 2022). Assuming that problems in the real world are more exacerbated than in the experimental setting, this experiment contributes to enhancing these abilities to face a complex cybersecurity environment and improving decision-making to build identifiable and stable processes or characterized as repeatable routines of investments in capabilities against cyber threats (Eisenhardt & Martin, 2000; Zollo & Winter, 2002). Additionally, the iterative learning process provided in this experiment brings attention to the participants in reinforcing abilities to an accurate organizational change, including new or modified ways of operating according to different systemic scenarios (Steininger et al., 2022). For example, operationalizations of information technologies embedded in dynamic capabilities range from exhaustive coverage of sensing, seizing, and transforming directly enabled by measures of data analytics (Torres et al., 2018) or resource transformation through internet of things (IoT) data (Côrte-Real et al., 2020).

Second, the experienced group was no more successful than the inexperienced group, indicating that a proactive stance toward investments in cybersecurity capability development is unrelated to experienced. In other words, more experience does not mean better decision making (Dukerich & Nichols, 1991; Fisher et al., 2003; Paese & Sniezek, 1991). In this sense, the issue of experience has not yet been addressed in the theory of dynamic capabilities in the IS research field as it has been in other research fields such as strategic management. Thus, we bring from the research field of strategic management that experienced individuals usually apply successful processes from the past in the present (K. G. Smith et al., 1991), seeking less exhaustive actions for decision making in investments. Therefore, this experiment contributes

to the literature by demonstrating that aspects of experienced information security may not be effective considering that "it is not enough to approach things in a logical and critical capacity, but one has to be willing to think unorthodoxly" (p. 131) (Steinmetz, 2015), when decisions are needed on cyber protection capabilities.

Third, when we compared the performance of participants in level one with level two, neither the experienced group nor the inexperienced group optimized their investments in cybersecurity capability development. This demonstrated that the unpredictability of cyber incidents impacted the performance of profit accumulation in the simulation. In literature, optimization demands searching for all logical possibilities (Evans, 2007). However, such logical possibilities are dependent on information sharing, which indicates that more investment in cybersecurity is followed by the formation of an information sharing environment (A. Yang et al., 2020). In other words, capabilities development and information are joint in cyber defense; however, the literature on dynamic capabilities does not cover information as part of organizational change or performance.

Finally, consistent with prior experiments in cybersecurity (Gupta et al., 2021; Jalali et al., 2019; Sharma et al., 2021), the findings of this experiment indicate that risk-averse cybersecurity behavior (Sharma et al., 2021) and security investment decisions ahead of attacks (Gupta et al., 2021) can be learned iteratively. Supposedly corroborating Gupta et al. (2021), individuals can invest relatively less when they are unaware of other participants' choices in advance.

4.5.2 Managerial Implications

This study offers valuable insights to entrepreneurs, managers, investors, and policymakers. First, it enables them to better understand that the learning process about CC investments needs to be continuous even for experienced individuals. The systems scenario at risks, affected and detected, are determinant to apply different efforts in many types of capabilities because information asymmetry and unsystematic cyber-risks are relevant to a data breach (Dong et al., 2023). With respect to learning iteratively, we find that virtual educational simulators are highly supportive and less costly than cyber-attacks. Therefore, entrepreneurs, managers, investors, and policymakers must be more aware that investing in simulations may be appropriate to enhance CC beyond technical certifications. We also suggest that simulation takes less effort in taking and publicizing immediate remedial actions and announces significant increases in budget to further improve cybersecurity capability. Additionally, some authors

(Demek & Kaplan, 2023) highlighted that investors' investment interest is lowest for a firm that previously indicates that cybersecurity risk management is a nonstrategic initiative. Therefore, simulators may provide insights to shift the way investors view cybersecurity regardless of the firm's approach so that they have taken it into account when assessing the value of a firm prior to making investment decisions.

Second, this experiment provides managers and entrepreneurs with information on how to handle investments in different capabilities during a cyber-attack event to prepare them for real situations that could cause concerns about negative valuation to the firms. Third, based on our evaluation, policymakers may also benefit from an iterative learning process applying simulations as a mandatory exercise before an investment in CC. It may allow legislators and regulators to realize the upsides of requiring firms to invest and report simulation activities against cyber-attacks to the public, thereby promoting more countries to begin to draft and implement learning notification laws. This study reveals that learning to invest in CC is a continuous process, never end, due to the relevant cyber-risk events reducing information asymmetry between the affected firms and their stakeholders, corroborating (Wessels et al., 2021), who highlighted that cybersecurity issues are ever-changing and require continuous investments.

4.6 FINAL CONSIDERATIONS

Using a simulation game tool, we could answer the research questions of whether there are differences between experienced and inexperienced groups in investing in capability development in cybersecurity, showing that the experienced group did not have much greater performance than the inexperienced group based on their proactive investment decisions. Additionally, the experiment also demonstrated that the process of learning in investments in CC can be achieved through a virtual iterative environment, answering the second research question.

The assumption for the unexpected performance from the groups is associated with uncertainty surrounding cyber incidents as present in the two levels of the simulation or in heuristics entrenched in decision-making, which was not the objective of our analysis. However, the majority of participants did not perform well in level two, suggesting that they were able to adopt proactive investments correlating the right capabilities to the "systems overview". On the other hand, the inexperienced group presented much more dynamism in the learning curve, adapting their investment strategies between the levels. Additionally, the results

demonstrated that the impact of trust in the simulation provoked a better perception of the importance of the simulator in the experiment. Therefore, simulations for better understanding the complexities of investing in CC are essential to improve decision-making in the future related to cyber incident scenarios, proving to be an effective training tool (Jalali et al., 2019).

In sum, this experiment also contributes to the social and economic fields. For social contribution, the simulator may be applied in any environmental condition to future entrepreneur development in cybersecurity. It can also contribute to the design of public policies that benefit more investments in this kind of technology. Economic contribution allows current and future entrepreneurs to invest time and resources in developing adequate dynamic capabilities in cybersecurity and to make assertive decisions about where, how, and when to invest.

4.6.1 Limitations and future studies

The general objective of this experiment was to provide iterative learning in the development of CC through random investments to reduce the cyber risks presented in the systems ecosystem of a fictitious company. The experiment was conducted in university laboratories, so to overcome this limitation, new applications of the experiment could be carried out using personal notebooks to detect disparities in the learning process. In other words, we analyze whether the participants would show differences in the investment pattern due to environmental influence. Another possibility would be to extend the simulation to study the long-term consequences of such an approach.

Additionally, we did not measure the participants' tolerance level for cyber risks or validate their experiences with questions pertinent to the topic. Thus, new research can add risk measurement indicators to reveal new decision-making patterns. The simulation model can also be improved by adjusting the simulator parameters to real cyber events and the inclusion of more cybersecurity experts in the sample. By assuming a simplicity that allows simulations, it would be interesting to add other complexities such as groups of simulations, simulations between groups of attackers and defenders with inverted positions from time to time, or even the definition of many different scenarios by the participants to get closer to reality.

4.7 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

Acquisti, A., & Grossklags, J. (2003). Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. 2nd Annual Workshop on Economics and Information Security-WEIS, 3, 1–27.

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

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

Aleroud, A., Abu-Shanab, E., Al-Aiad, A., & Alshboul, Y. (2020). An examination of susceptibility to spear phishing cyber-attacks in non-English speaking communities. Journal of Information Security and Applications, 55, 102614. https://doi.org/10.1016/j.jisa.2020.102614

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

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

Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. Computers & Security, 59, 9–25. https://doi.org/10.1016/j.cose.2016.02.007

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

Beuran, R., Vykopal, J., Belajová, D., Čeleda, P., Tan, Y., & Shinoda, Y. (2023). Capability Assessment Methodology and Comparative Analysis of Cybersecurity Training Platforms. Computers & Security, 128, 103120. https://doi.org/10.1016/j.cose.2023.103120

Bitzer, M., Häckel, B., Leuthe, D., Ott, J., Stahl, B., & Strobel, J. (2023). Managing the Inevitable – A Maturity Model to Establish Incident Response Management Capabilities. Computers & Security, 125, 103050. https://doi.org/10.1016/j.cose.2022.103050

Bowen, B. M., Devarajan, R., & Stolfo, S. (2011). Measuring the human factor of cyber security. 2011 IEEE International Conference on Technologies for Homeland Security (HST), 230–235. https://doi.org/10.1109/THS.2011.6107876

Bulgurcu, Cavusoglu, & Benbasat. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, 34(3), 523. https://doi.org/10.2307/25750690

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

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. Journal of Information Security and Applications, 42, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

Catal, C., Ozcan, A., Donmez, E., & Kasif, A. (2023). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. Education and Information Technologies, 28(2), 1809–1831. https://doi.org/10.1007/s10639-022-11261-8

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

Chatterjee, S., & Thekdi, S. (2020). An iterative learning and inference approach to managing dynamic cyber vulnerabilities of complex systems. Reliability Engineering & System Safety, 193, 106664. https://doi.org/10.1016/j.ress.2019.106664

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

Côrte-Real, N., Ruivo, P., & Oliveira, T. (2020). Leveraging internet of things and big data analytics initiatives in European and American firms: Is data quality a way to extract business value? Information & Management, 57(1), 103141. https://doi.org/10.1016/j.im.2019.01.003

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

Daniel, C., Mullarkey, M., & Agrawal, M. (2022). RQ Labs: A Cybersecurity Workforce Skills Development Framework. Information Systems Frontiers. https://doi.org/10.1007/s10796-022-10332-y

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

Demek, K. C., & Kaplan, S. E. (2023). Cybersecurity breaches and investors' interest in the firm as an investment. International Journal of Accounting Information Systems, 49, 100616. https://doi.org/10.1016/j.accinf.2023.100616

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

Dinkova, M., El-Dardiry, R., & Overvest, B. (2023). Should firms invest more in cybersecurity? Small Business Economics. https://doi.org/10.1007/s11187-023-00803-0

Disparte, D., & Furlow, C. (2017). The best cybersecurity investment you can make is better training. Harvard Business Review, 5.

Dong, T., Zhu, S., Oliveira, M., & Luo, X. (Robert). (2023). Making better IS security investment decisions: Discovering the cost of data breach announcements during the COVID-19 pandemic. Industrial Management & Data Systems, 123(2), 630–652. https://doi.org/10.1108/IMDS-06-2022-0376

Dukerich, J. M., & Nichols, M. L. (1991). Causal information search in managerial decision making. Organizational Behavior and Human Decision Processes, 50(1), 106–122. https://doi.org/10.1016/0749-5978(91)90036-S

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

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

Ekelund, S., & Iskoujina, Z. (2019). Cybersecurity economics – balancing operational security spending. Information Technology & People, 32(5), 1318–1342. https://doi.org/10.1108/ITP-05-2018-0252

Evans, J. S. B. T. (2007). Hypothetical thinking: Dual processes in reasoning and judgement (1st ed). Psychology Press.

Fagade, T., Maraslis, K., & Tryfonas, T. (2017). Towards effective cybersecurity resource allocation: The Monte Carlo predictive modelling approach. International Journal of Critical Infrastructures, 13(2/3), 152. https://doi.org/10.1504/IJCIS.2017.088235

Fernandez De Arroyabe, I., Arranz, C. F. A., Arroyabe, M. F., & Fernandez De Arroyabe, J. C. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. Computers & Security, 124, 102954. https://doi.org/10.1016/j.cose.2022.102954

Fisher, C. W., Chengalur-Smith, I., & Ballou, D. P. (2003). The Impact of Experience and Time on the Use of Data Quality Information in Decision Making. Information Systems Research, 14(2), 170–188. https://doi.org/10.1287/isre.14.2.170.16017

Fleischman, G. M., Valentine, S. R., Curtis, M. B., & Mohapatra, P. S. (2023). The Influence of Ethical Beliefs and Attitudes, Norms, and Prior Outcomes on Cybersecurity Investment Decisions. Business & Society, 62(3), 488–529. https://doi.org/10.1177/00076503221110156

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

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

Gupta, R., Biswas, B., Biswas, I., & Sana, S. S. (2021). Firm investment decisions for information security under a fuzzy environment: A game-theoretic approach. Information & Computer Security, 29(1), 73–104. https://doi.org/10.1108/ICS-02-2020-0028

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

Hsu, C., Lee, J.-N., & Straub, D. W. (2012). Institutional Influences on Information Systems Security Innovations. Information Systems Research, 23(3-part-2), 918–939. https://doi.org/10.1287/isre.1110.0393

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

Hwang, M. I., & Helser, S. (2022). Cybersecurity educational games: A theoretical framework. Information & Computer Security, 30(2), 225–242. https://doi.org/10.1108/ICS-10-2020-0173

IBM Security. (2023). Cost of a Data Breach Report 2023 (p. 1–78). IBM Security; pdf. https://www.ibm.com/reports/data-breach

Jalali, M. S. (2014). How Individuals Weigh Their Previous Estimates to Make a New Estimate in the Presence or Absence of Social Influence. Em W. G. Kennedy, N. Agarwal, & S. J. Yang (Orgs.), Social Computing, Behavioral-Cultural Modeling and Prediction (Vol. 8393, p. 67–74). Springer International Publishing. https://doi.org/10.1007/978-3-319-05579-4_9

Jalali, M. S., Ashouri, A., Herrera-Restrepo, O., & Zhang, H. (2016). Information diffusion through social networks: The case of an online petition. Expert Systems with Applications, 44, 187–197. https://doi.org/10.1016/j.eswa.2015.09.014

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

Kalderemidis, I., Farao, A., Bountakas, P., Panda, S., & Xenakis, C. (2022). GTM: Game Theoretic Methodology for optimal cybersecurity defending strategies and investments. Proceedings of the 17th International Conference on Availability, Reliability and Security, 1–9. https://doi.org/10.1145/3538969.3544431

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

Karagiannis, S., & Magkos, E. (2021). Adapting CTF challenges into virtual cybersecurity learning environments. Information & Computer Security, 29(1), 105–132. https://doi.org/10.1108/ICS-04-2019-0050

Khalid Khan, S., Shiwakoti, N., & Stasinopoulos, P. (2022). A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles. Accident Analysis & Prevention, 165, 106515. https://doi.org/10.1016/j.aap.2021.106515

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

Madnick, S., Jalali, M. S., Siegel, M., Lee, Y., Strong, D., Wang, R., Ang, W. H., Deng, V., & Mistree, D. (2017). Measuring Stakeholders' Perceptions of Cybersecurity for Renewable Energy Systems. Em W. L. Woon, Z. Aung, O. Kramer, & S. Madnick (Orgs.), Data Analytics for Renewable Energy Integration (Vol. 10097, p. 67–77). Springer International Publishing. https://doi.org/10.1007/978-3-319-50947-1_7

Master, A., Hamilton, G., & Dietz, J. E. (2022). Optimizing Cybersecurity Budgets with AttackSimulation. 2022 IEEE International Symposium on Technologies for Homeland Security (HST), 1–7. https://doi.org/10.1109/HST56032.2022.10024984

McClain, J., Silva, A., Emmanuel, G., Anderson, B., Nauer, K., Abbott, R., & Forsythe, C. (2015). Human Performance Factors in Cyber Security Forensic Analysis. Procedia Manufacturing, 3, 5301–5307. https://doi.org/10.1016/j.promfg.2015.07.621

McFarland, L., Milstein, B., Hirsch, G., Homer, J., Andersen, D., Irving, R., Reineke, E., Niles, R. D., Cawvey, E., Desai, A., & MacDonald, R. (2016). NASPAA Student Simulation Competition: Reforming the U.S. Health Care System Within a Simulated Environment. Journal of Public Affairs Education, 22(3), 363–380. https://doi.org/10.1080/15236803.2016.12002253

Meland, P. H., Bernsmed, K., Frøystad, C., Li, J., & Sindre, G. (2019). An experimental evaluation of bow-tie analysis for security. Information & Computer Security, 27(4), 536–561. https://doi.org/10.1108/ICS-11-2018-0132

Mingers, J., & Standing, C. (2020). A Framework for Validating Information Systems Research Based on a Pluralist Account of Truth and Correctness. Journal of the Association for Information Systems, 117–151. https://doi.org/10.17705/1jais.00594

Morellato, L. P. C., Alberti, L. F., & Hudson, I. L. (2010). Applications of Circular Statistics in Plant Phenology: A Case Studies Approach. Em Phenological Research (p. 339–359). Springer Netherlands. https://doi.org/10.1007/978-90-481-3335-2_16

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

OliveiraJr, E., Zorzo, A. F., & Neu, C. V. (2020). Towards a conceptual model for promoting digital forensics experiments. Forensic Science International: Digital Investigation, 35, 301014. https://doi.org/10.1016/j.fsidi.2020.301014

Paese, P. W., & Sniezek, J. A. (1991). Influences on the appropriateness of confidence in judgment: Practice, effort, information, and decision-making. Organizational Behavior and Human Decision Processes, 48(1), 100–130. https://doi.org/10.1016/0749-5978(91)90008-H

Pentland, S. J., Twyman, N. W., Burgoon, J. K., Nunamaker, J. F., & Diller, C. B. R. (2017). A Video-Based Screening System for Automated Risk Assessment Using Nuanced Facial Features. Journal of Management Information Systems, 34(4), 970–993. https://doi.org/10.1080/07421222.2017.1393304

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

Pigola, A. (2023). Enhancing Capabilities Development in Cybersecurity: Evidence from an experiment. Harvard Dataverse. https://doi.org/10.7910/DVN/U6SV8J,

Rahmandad, H. (2012). Impact of Growth Opportunities and Competition on Firm-Level Capability Development Trade-offs. Organization Science, 23(1), 138–154. https://doi.org/10.1287/orsc.1100.0628

Rahmandad, H., & Weiss, D. M. (2009). Dynamics of concurrent software development: H. Rahmandada and D. M. Weiss: Dynamics of Concurrent Software Development. System Dynamics Review, 25(3), 224–249. https://doi.org/10.1002/sdr.425

Robinson, S. (2008). Conceptual modelling for simulation Part I: Definition and requirements. Journal of the Operational Research Society, 59(3), 278–290. https://doi.org/10.1057/palgrave.jors.2602368

Sangari, S., Dallal, E., & Whitman, M. (2023). Modeling reporting delays in cyber incidents: An industry-level comparison. International Journal of Information Security, 22(1), 63–76. https://doi.org/10.1007/s10207-022-00623-5

Sewak, M., Sahay, S. K., & Rathore, H. (2022). Deep Reinforcement Learning in the Advanced Cybersecurity Threat Detection and Protection. Information Systems Frontiers. https://doi.org/10.1007/s10796-022-10333-x

Shaikh, F. A., & Siponen, M. (2023). Organizational Learning from Cybersecurity Performance: Effects on Cybersecurity Investment Decisions. Information Systems Frontiers. https://doi.org/10.1007/s10796-023-10404-7

Sharma, K., Zhan, X., Nah, F. F.-H., Siau, K., & Cheng, M. X. (2021). Impact of digital nudging on information security behavior: An experimental study on framing and priming in cybersecurity. Organizational Cybersecurity Journal: Practice, Process and People, 1(1), 69–91. https://doi.org/10.1108/OCJ-03-2021-0009

Shreeve, B., Gralha, C., Rashid, A., Araújo, J., & Goulão, M. (2023). Making Sense of the Unknown: How Managers Make Cyber Security Decisions. ACM Transactions on Software Engineering and Methodology, 32(4), 1–33. https://doi.org/10.1145/3548682

Smith, K. G., Grimm, C. M., Gannon, M. J., & Chen, M.-J. (1991). Organizational Information Processing, Competitive Responses, and Performance in the U.S. Domestic Airline Industry. Academy of Management Journal, 34(1), 60–85. https://doi.org/10.2307/256302

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

Sterman, J. D. (2001). System Dynamics Modeling: Tools for Learning in a Complex World. California Management Review, 43(4), 8–25. https://doi.org/10.2307/41166098

Sterman, J. D., Franck, T., Fiddaman, T., Jones, A., McCauley, S., Rice, P., Sawin, E., Siegel, L., & Rooney-Varga, J. N. (2015). World Climate: A Role-Play Simulation of Climate Negotiations. Simulation & Gaming, 46(3–4), 348–382. https://doi.org/10.1177/1046878113514935

Sull, D. N., & Eisenhardt, K. M. (2015). Simple rules: How to thrive in a complex world. John Murray.

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., 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

Torres, R., Sidorova, A., & Jones, M. C. (2018). Enabling firm performance through business intelligence and analytics: A dynamic capabilities perspective. Information & Management, 55(7), 822–839. https://doi.org/10.1016/j.im.2018.03.010

Van Der Kleij, R., Schraagen, J. M., Cadet, B., & Young, H. (2022). Developing decision support for cybersecurity threat and incident managers. Computers & Security, 113, 102535. https://doi.org/10.1016/j.cose.2021.102535

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, J., Gupta, M., & Rao, H. R. (2015). Insider Threats in a Financial Institution. MIS Quarterly, 39(1), 91–112. JSTOR. https://www.jstor.org/stable/26628342

Wessels, M., Van Den Brink, P., Verburgh, T., Cadet, B., & Van Ruijven, T. (2021). Understanding incentives for cybersecurity investments: Development and application of a typology. Digital Business, 1(2), 100014. https://doi.org/10.1016/j.digbus.2021.100014

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. MIS quarterly, 1–20. https://www.jstor.org/stable/43825935

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. Journal of the American Society for Information Science and Technology, 59(4), 662–674. https://doi.org/10.1002/asi.20779

Xu, F., Luo, X. (Robert), Zhang, H., Liu, S., & Huang, W. (Wayne). (2019). Do Strategy and Timing in IT Security Investments Matter? An Empirical Investigation of the Alignment Effect. Information Systems Frontiers, 21(5), 1069–1083. https://doi.org/10.1007/s10796-017-9807-6

Xu, L., Li, Y., Lin, Y., Tang, C., & Yao, Q. (2023). Supply chain cybersecurity investments with interdependent risks under different information exchange modes. International Journal of Production Research, 1–26. https://doi.org/10.1080/00207543.2023.2206923

Yamagishi, T., & Yamagishi, M. (1994). Trust and commitment in the United States and Japan. Motivation and Emotion, 18(2), 129–166. https://doi.org/10.1007/BF02249397

Yang, A., Kwon, Y. J., & Lee, S.-Y. T. (2020). The impact of information sharing legislation on cybersecurity industry. Industrial Management & Data Systems, 120(9), 1777–1794. https://doi.org/10.1108/IMDS-10-2019-0536

Yang, M. M., Jiang, H., & Gary, M. S. (2016). Challenging learning goals improve performance in dynamically complex microworld simulations. System Dynamics Review, 32(3–4), 204–232. https://doi.org/10.1002/sdr.1559

Zacharis, A., & Patsakis, C. (2023). AiCEF: An AI-assisted cyber exercise content generation framework using named entity recognition. International Journal of Information Security, 22(5), 1333–1354. https://doi.org/10.1007/s10207-023-00693-z

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

Zhang, L., Zhu, J., & Liu, Q. (2012). A meta-analysis of mobile commerce adoption and the moderating effect of culture. Computers in Human Behavior, 28(5), 1902–1911. https://doi.org/10.1016/j.chb.2012.05.008

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

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems, 62(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

4.8 APPENDIX F. DETAILED PROCESS OF THE OPERACIONALIZATION OF THE EXPERIMENT

The process of experiment started identifying professors into the institutions of education interested in cybersecurity theme in their disciplines. After explaining the reasons behind the experiment, the professors were introduced to the simulation process to make sure that the content of the experiment would be aligned with the expectation of learning to the students. Additionally, the identification of appropriate laboratory in each institution that could support the simulator access through computers foregone the decision of acceptance of applying the experiment. Figure F1 provides evidence of the laboratories of the institutions which offer a control environment to perform the experiment.

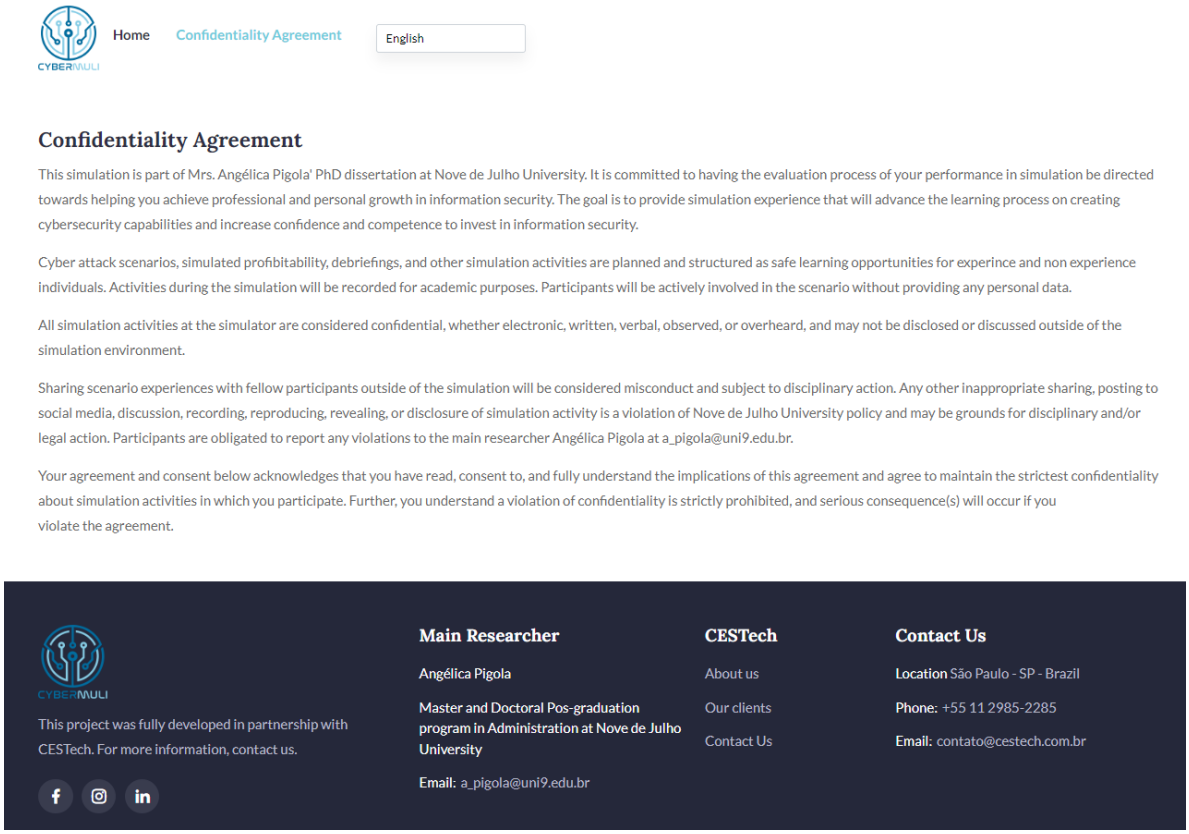
Figure F1. Laboratories of the institutions of education

Note. Data gathering occurred in two different universities in three distinctive locations and five groups of students in May and June 2023.

Furthermore, ethical issues was discussed and explained to each institution in order to guarantee appropriate privacy of the participants. Considering that the simulator did not take any personal data an ethical committee approval was dispensable. However, regardless the experiment did not take any personal information from the participants and each institution provide its own privacy protection into the computers, the simulator provided a confidentiality

agreement which each participant declared your acceptance to participate in the experiment. Figure F2 provides a screenshot of the confidentiality agreement.

Figure F2. Confidentiality Agreement of the simulator



Before starting the data collection through the simulation, each participant received written instructions into the simulator and an introduction of cybersecurity scenario through a presentation that offered the necessary background of cybersecurity capabilities together with the introductions already in place inside the simulator. Figure F3 provides a screenshot of instructions into the simulator. The professors who supported this experiment provided the benefit of half a point in the final grade of the discipline to the participants who finalize the experiment until the end. Furthermore, the simulator contemplated to each participant the analysis of its own performance in the simulation by a report in each level completed. Figure F4 provides a screenshot of the report into the simulator. These activities and data provided were relevant to bring attention to the students. Each experiment took no longer than 2 hours. In summary, participants were physically tested in different locations and despite social influences, they were not allowed to discuss or reveal their results at any time during the simulation.

Figure F3. Instructions into the simulator

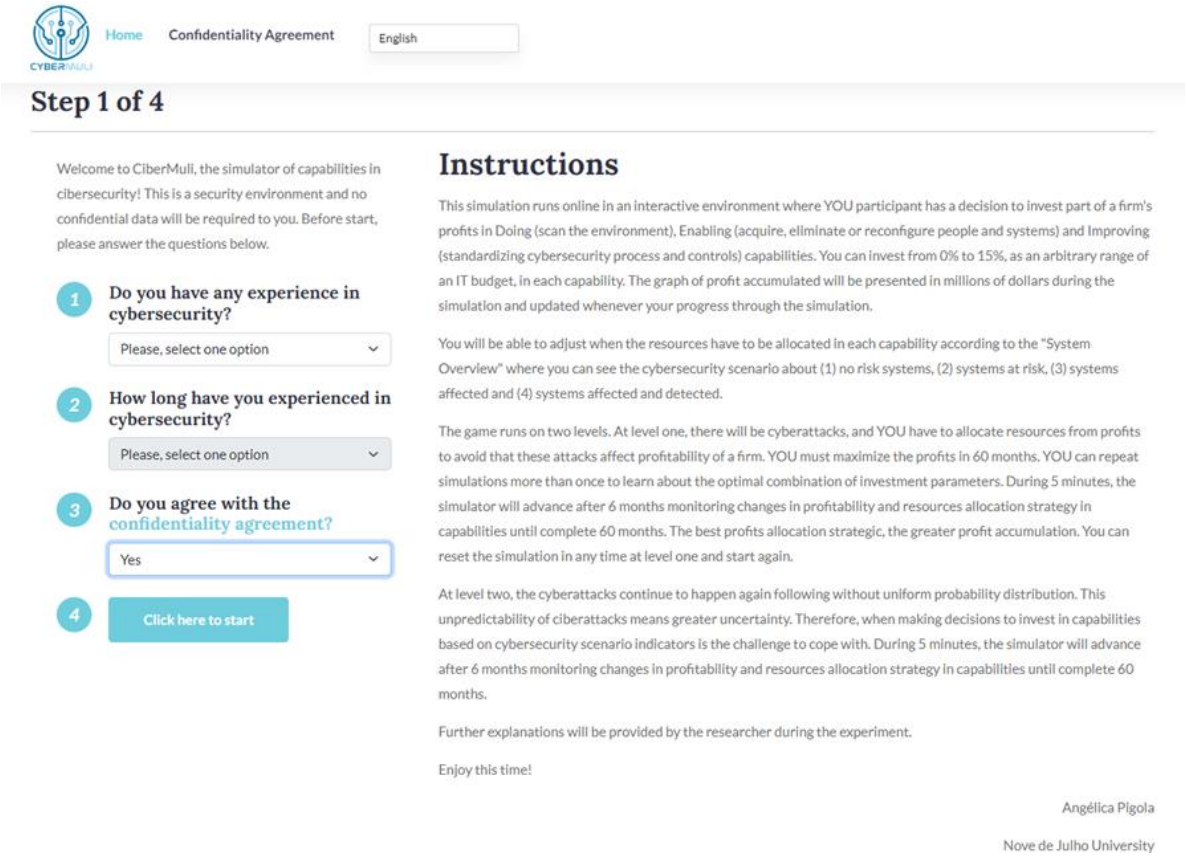
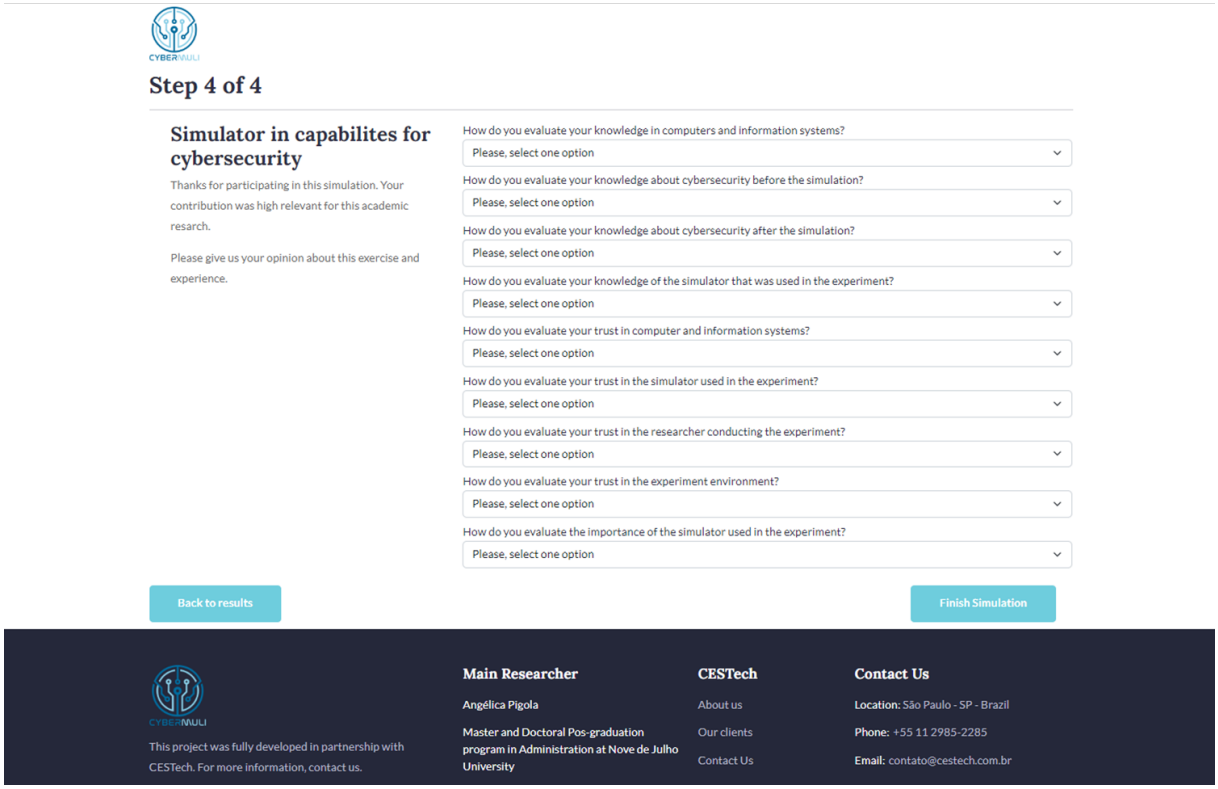


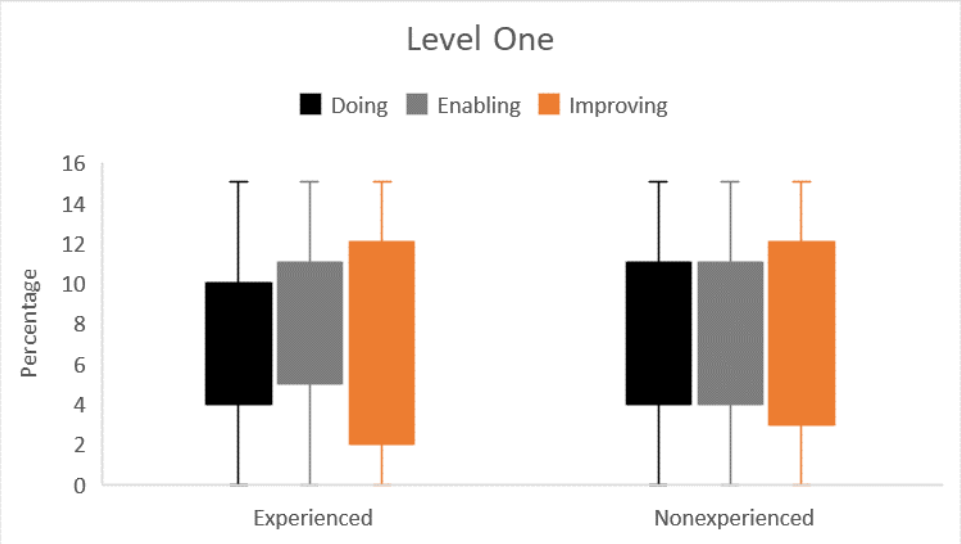
Figure F4. Final report of performance into the simulator

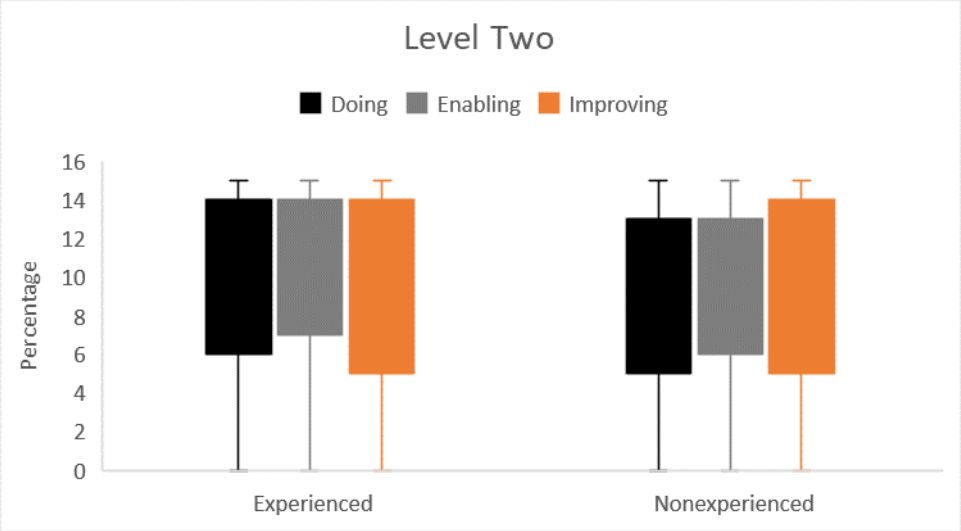
In level one, participants had an opportunity to run the simulation many times as a practice mode and raise questions about doubts of the simulator. Participants were not aware of the difference between the two levels until the results were presented at the end of the experiment through the final report (Figure F4). The simplicity of the simulator helped to better explain the process to the participants and analyze the decision-making behavior of resource allocation dynamics. It also allows participants to better engage with the simulator. At the end of the simulation, participants answered questions about the trust and knowledge impact after the experiment. Figure F5 shows a screenshot of the survey into the simulator.

Figure F5. Survey about the simulator



4.9 APPENDIX G. LEVEL OF INVESTMENTS IN CYBERSECURITY CAPABILITIES





4.10 APPENDIX H. SURVEY INSTRUMENT FACTOR LOADINGS AND STATISTICS

	Survey Instrument	Mean	Std. Dev.	W	Loadings	Std. Error	z value
SRK1	How do you evaluate your knowledge in computers and information systems?	2.807	1.002	0.886	0.789	0.085	9.300
SRK2	How do you evaluate your knowledge about cybersecurity before the simulation?	2.092	1.041	0.846	0.573	0.095	6.234
SRK3	How do you evaluate your knowledge about cybersecurity after the simulation?	3.067	0.972	0.885	0.757	0.083	8.820
SRK4	How do you evaluate your knowledge of the simulator that was used in the experiment?	2.924	1.059	0.911	0.540	0.098	5.807
TRI1	How do you evaluate your trust in computers and information systems?	2.992	1.046	0.906	0.669	0.096	7.292
TRI2	How do you evaluate your trust in the simulator used in the experiment?	3.303	1.117	0.895	0.663	0.102	7.204
TRI3	How do you evaluate your trust in the researcher conducting the experiment?	3.790	1.156	0.850	0.564	0.109	5.942
TRI4	How do you evaluate your trust in the experiment environment?	3.630	1.096	0.869	0.606	0.102	6.468
EOS	How do you evaluate the importance of the simulator used in the experiment?	4.328	0.940	0.711			

Note. Shapiro–Wilk Normality Test (W); p value <.001 for all indices. Bootstrap samples were successful on 5,000 samples; composite reliability above 0.769; average variance extracted above 0.472

5 FINAL CONSIDERATION

In this section, I revisit the most important findings and contributions highlighted throughout studies one (meta-synthesis) and two (survey) of the dissertation (Table 20). Moreover, I describe how these findings advanced the theories used and related fields. Through a postpositivist-oriented analysis focused on the findings, by answering the main research question, in which level do dynamic capabilities affect cybersecurity intelligence for business change, performance, and innovations? I conclude that dynamic capabilities in cybersecurity have the potential to shape future cybersecurity intelligence, even though the current involvement of academics and practitioners has emphasized more technical aspects of cybersecurity than management ones such as the planning, communication, and engagement of stakeholders.

Firms may mobilize further resources and institutional collaboration available to reach out to higher levels of dynamic capabilities development in cybersecurity. Those involved in cybersecurity events will invest more resources to find strategic ways to be persuasive in the planning they would like to portray for information security. Across the studies, our results suggest the following:

The rise of DCCI is inevitable in the process of the cybersecurity phenomena based on the human capabilities chain. Dynamic capabilities in cybersecurity generated a level of cybersecurity intelligence in the businesses in question (at least in innovation, change, or performance). Moving from theory to practice, the visibility of the DCCI can be introduced and incorporated as a complementary view from the perspective of dynamic capabilities. Discussions show that understanding and adhering to the applicability of each DCCI can help firms learn more effectively about cybersecurity practices, processes, and abilities. The journey to develop and achieve DCCI will certainly include unforeseen challenges, and critical adjustments will aid the implementation of the DCCI framework.

Dynamic capabilities in cybersecurity enable firms to build their CI. However, not all capabilities directly impact CI development, and appropriately identifying what processes and abilities are required for cybersecurity business requirements is necessary. Capabilities indicated in the DCCI framework may be considered dynamic capabilities because they influence changing and performing CI and how they are classified according to dynamic capability microfoundations. The findings reveal the relevance of cybersecurity engineering and improvements in cybersecurity activities for developing CI. It also pointed out that

managing cybersecurity is more relevant in planning activities than adjusting team structure to business requirements.

Investments in cybersecurity capabilities must be learnt iteratively regardless of the experience of individuals. The assumption for the unexpected performance of the groups is associated with uncertainty surrounding cyber incidents or in heuristics entrenched in decision-making which was not the objective of this analysis and might be explored in the future. Additionally, simulations for better understanding the complexities of investing in cybersecurity capabilities are essential to improve decision-making in the future related to cyber incident scenarios, proving to be an effective training tool.

This dissertation contributes to the social, scientific, and economic fields. For s*ocial contribution,* the research proposal amplifies the understanding of the relevance of dynamic cybersecurity capacity development related to innovation technologies for cybernetic protection, and it will allow the design of new academic and practical disciplines for business development in cybersecurity. It can also contribute to the design of public policies that benefit more investments in this kind of technology. For *scientific contribution,* the topic of cybersecurity requires attention given to new theories and theoretical model development that meet business demands in terms of new technologies. It provides greater cybersecurity consciousness for firms and public institutions to require dynamic cybersecurity capabilities. The methods developed will favorably contribute to advancing the dynamic capabilities and cyber innovation literature. For *economic contribution,* this dissertation allows current and future entrepreneurs to invest time and resources in developing adequate dynamic capabilities in cybersecurity, as well as make assertive decisions about where, how, and when to invest.

This study also makes the following contributions: (1) presenting a theoretical decision-making model for developing dynamic cybersecurity capabilities for cyberattack predictability; (2) developing scientific articles that provide entrepreneurs and technology experts with an understanding of how to develop dynamic cybersecurity capabilities that foster the development of cybersecurity technologies and/or better management of factors related to virtual protection; (3) designing curricular models for training and education on cybersecurity that can develop dynamic cybersecurity capabilities aimed at developing or managing virtual protection technologies at the national level; and (4) integrating this field of study as a strategic factor in organizational decision-making through a new theoretical approach to be investigated.

Table 20. Contributory Matrix

MAIN RESEACH QUESTION **At which level do cybersecurity capabilities development and investments affect cybersecurity intelligence in business?**			
MAIN GOAL Demonstrating that cybersecurity capabilities are paramount in cyber risks mitigation, cyber uncertainties reduction, and cyber innovations. The development of these capabilities directly impacts cybersecurity intelligence, and the investments can be learnt iteratively.			
PARTICULAR CONCLUSION			
Summary of results	Contributions to the advancement of knowledge	Limitations	Future Agenda
STUDY 1 Dynamics Capabilities in Cybersecurity Intelligence: A Meta-Synthesis to Enhance Protection Against Cyber Threats	The rise of Dynamic Capabilities in Cybersecurity Intelligence is inevitable in the process of the cybersecurity phenomena based on the human capabilities chain.	Case studies, as the only sample of choice, given the difficulty to produce large and multiple different methods, also have to do with external validity, which means the generality of the results with respect to a specific population.	Applying new model measurements in different contexts and under other theories. Online tools development to explain dynamic capabilities in various contexts (e.g., large enterprises, supply chain, different regions, and industries) could be included.
STUDY 2 Dynamic Capabilities in Cybersecurity: Empirical Evidence to Enhance Management Against Cyber threats	A new instrument of measurement to Dynamic capabilities in cybersecurity that enable firms to build their Cybersecurity Intelligence. Evidencing that the technical aspects (Doing and Improving) are more considered to build cybersecurity intelligence than management aspects (Enabling and Managing).	The variables may offer limited insights into the drivers of information security. This study provides data from a single survey completed by multiple respondents. Even using several techniques when developing the survey to prevent the endogeneity of the variables, the instrument applied does not capture all capabilities for cybersecurity. The measures are open to interpretation and might not reflect the actual rate of dynamic capabilities in cybersecurity intelligence.	Questioning more about managing external stakeholders and validating the model in other different contexts, especially in firms in the technological industry. Additionally, quantifying all variables more rigorously to improve the model.
STUDY 3 Enhancing Cybersecurity Capabilities Investments: Evidence from an experiment	It contributes to enhancing abilities to face a complex cybersecurity environment and improving decision-making to build identifiable and stable processes or characterized as repeatable routines of investments in capabilities against cyber threats. The iterative learning process brings attention in reinforcing abilities to an accurate organizational change, including new or modified ways of operating according to different systemic scenarios	The experiment was conducted in university laboratories, so to overcome this limitation, new applications of the experiment could be carried out using personal notebooks to detect disparities in the learning process. Additionally, we did not measure the participants' tolerance level for cyber risks or validate their experiences with questions pertinent to the topic.	New research can add risk measurement indicators to reveal new decision-making patterns. It also be improved by adjusting the simulator parameters to real cyber events and the inclusion of more cybersecurity experts in the sample. It would be interesting to add other complexities such as groups of simulations, simulations between groups of attackers and defenders with inverted positions, or even the definition of many different scenarios by the participants to get closer to reality.
INTEGRATING CONCLUSION			
Findings reveals that without capabilities in cybersecurity firms are likely unable to adapt their strategy to increasingly enhance their cybersecurity intelligence. By developing these capabilities firms are more likely to consider the changes in the environment in which they are networking. When there is development in cybersecurity capabilities, firms are more likely to be less vulnerable, especially if they are under cyberattacks. It seems to be obvious, but it is not, because neglected behaviors still exist in business environments. Therefore, firms should pay close attention to their networks environments to develop appropriate cybersecurity capabilities according to their context-specifics. Additionally, the positive aspects for firms is that investments in cybersecurity capabilities can be learnt proactively and iteratively in a certain level.			

Source. Da Costa et al. (2019).

5.1 REFERENCES

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

Adomavicius, Bockstedt, Gupta, & Kauffman. (2008). Making Sense of Technology Trends in the Information Technology Landscape: A Design Science Approach. *MIS Quarterly*, *32*(4), 779. https://doi.org/10.2307/25148872

Bag, S., Gupta, S., & Luo, Z. (2020). Examining the role of logistics 4.0 enabled dynamic capabilities on firm performance. *The International Journal of Logistics Management*, *31*(3), 607–628. https://doi.org/10.1108/IJLM-11-2019-0311

Baghaei Lakeh, A., & Ghaffarzadegan, N. (2016). The dual-process theory and understanding of stocks and flows: The Dual-Process Theory and Understanding of Stocks and Flows. *System Dynamics Review*, *32*(3–4), 309–331. https://doi.org/10.1002/sdr.1566

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. *Journal of Management*, *17*(1), 99–120. https://doi.org/10.1177/014920639101700108

Baskerville, R. (1989). Logical controls specification: An approach to information systems security. *Systems development for human progress*, *25*(4), 241–255.

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

Biesta, G. (2010). Pragmatism and the philosophical foundations of mixed methods research. *Sage handbook of mixed methods in social and behavioral research*, *2*, 95–118.

Bose, R., & Luo, X. (2014). Investigating security investment impact on firm performance. *International Journal of Accounting & Information Management*, *22*(3), 194–208. https://doi.org/10.1108/IJAIM-04-2014-0026

Burrell, G., & Morgan, G. (2017). *Sociological Paradigms and Organisational Analysis* (0 ed). Routledge. https://doi.org/10.4324/9781315242804

Butler, S. A. (2002). Security attribute evaluation method: A cost-benefit approach. *Proceedings of the 24th International Conference on Software Engineering - ICSE '02*, 232. https://doi.org/10.1145/581339.581370

Carlton, M., Levy, Y., & Ramim, M. (2019). Mitigating cyber-attacks through the measurement of non-IT professionals' cybersecurity skills. *Information & Computer Security*, *27*(1), 101–121. https://doi.org/10.1108/ICS-11-2016-0088

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., Cavusoglu, H., Son, J.-Y., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management*, *52*(4), 385–400. https://doi.org/10.1016/j.im.2014.12.004

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

Chai, D. S., & Dirani, K. (2018). The dimensions of the learning organization questionnaire (DLOQ): A validation study in the Lebanese context. *The Learning Organization*, *25*(5), 320–330. https://doi.org/10.1108/TLO-03-2016-0017

Chai, S., Kim, M., & Rao, H. R. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems*, *50*(4), 651–661. https://doi.org/10.1016/j.dss.2010.08.017

Chatfield, A. T., & Reddick, C. G. (2019). A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government. *Government Information Quarterly*, *36*(2), 346–357. https://doi.org/10.1016/j.giq.2018.09.007

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

Christensen, C. M. (1997). *The innovator's dilemma: When new technologies cause great firms to fail*. http://proquest.safaribooksonline.com/?fpi=9781633691797

Creswell, J. W., & Clark, V. L. P. (2018). *Designing and conducting mixed methods research* (Third edition, international student edition). Sage.

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

Da Costa, P. R., Ramos, H. R., & Pedron, C. D. (2019). Alternative Structure Proposition for PhD Thesis from Multiple Studies. *Revista Ibero-Americana de Estratégia*, *18*(2), 155–170. https://doi.org/10.5585/riae.v18i2.15156

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., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal*, *11*(2), 127–153. https://doi.org/10.1046/j.1365-2575.2001.00099.x

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

Dierickx, I., & Cool, K. (1989). Asset Stock Accumulation and Sustainability of Competitive Advantage. *Management Science*, *35*(12), 1504–1511. https://doi.org/10.1287/mnsc.35.12.1504

Eggers, J. P., & Kaplan, S. (2009). Cognition and Renewal: Comparing CEO and Organizational Effects on Incumbent Adaptation to Technical Change. *Organization Science*, *20*(2), 461–477. https://doi.org/10.1287/orsc.1080.0401

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

Forbes (2023), *Brazil Is The World's Second Most Vulnerable Country To Cyberattacks*. Retrieved from https://www.forbes.com/sites/angelicamarideoliveira/2023/09/27/brazil-is-the-worlds-second-most-vulnerable-country-to-cyberattacks/?sh=4bdd7db927a4#open-web-0 in December 05th, 2023.

Fox, N. J. (2008). Post-positivism. *The SAGE encyclopedia of qualitative research methods*, *2*, 659–664.

Gonzalez, C., Qi, L., Sriwattanakomen, N., & Chrabaszcz, J. (2017). Graphical features of flow behavior and the stock and flow failure: Behavior-over-time graphs and Stock and Flow Failure. *System Dynamics Review*, *33*(1), 59–70. https://doi.org/10.1002/sdr.1570

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, *5*(4), 438–457. https://doi.org/10.1145/581271.581274

Grant, R. M. (1996). Toward a knowledge-based theory of the firm: Knowledge-based Theory of the Firm. *Strategic Management Journal*, *17*(S2), 109–122. https://doi.org/10.1002/smj.4250171110

Hall, J. N. (2013). Pragmatism, Evidence, and Mixed Methods Evaluation. *New Directions for Evaluation*, *2013*(138), 15–26. https://doi.org/10.1002/ev.20054

Havakhor, T., Rahman, M. S., & Zhang, T. (2020). *Cybersecurity Investments and the Cost of Capital*. SSRN. https://weis2020.econinfosec.org/wp-content/uploads/sites/8/2020/06/weis20-final16.pdf

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

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

Jahja, A. (2017). *Quality in Qualitative Research*. Perbanas Institute. https://dosen.perbanas.id/quality-in-quantitative-qualitative-research/

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

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems*, *25*(3), 231–251. https://doi.org/10.1057/ejis.2015.15

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

Kelemen, M., & Rumens, N. (2008). *An introduction to critical management research*. SAGE.

Ketokivi, M., & Mantere, S. (2010). Two Strategies for Inductive Reasoning in Organizational Research. *Academy of Management Review*, *35*(2), 315–333. https://doi.org/10.5465/amr.35.2.zok315

Komljenovic, D., Gaha, M., Abdul-Nour, G., Langheit, C., & Bourgeois, M. (2016). Risks of extreme and rare events in Asset Management. *Safety Science*, *88*, 129–145. https://doi.org/10.1016/j.ssci.2016.05.004

Kosutic, D., & Pigni, F. (2022). Cybersecurity: Investing for competitive outcomes. *Journal of Business Strategy*, *43*(1), 28–36. https://doi.org/10.1108/JBS-06-2020-0116

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

Krutilla, K., Alexeev, A., Jardine, E., & Good, D. (2021). The Benefits and Costs of Cybersecurity Risk Reduction: A Dynamic Extension of the Gordon and Loeb Model. *Risk Analysis*, *41*(10), 1795–1808. https://doi.org/10.1111/risa.13713

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

Li, X. (2021). Decision making of optimal investment in information security for complementary enterprises based on game theory. *Technology Analysis and Strategic Management*, *33*(7), 755–769. https://doi.org/10.1080/09537325.2020.1841158

Madnick, S., Jalali, M. S., Siegel, M., Lee, Y., Strong, D., Wang, R., Ang, W. H., Deng, V., & Mistree, D. (2017). Measuring Stakeholders' Perceptions of Cybersecurity for Renewable Energy Systems. In W. L. Woon, Z. Aung, O. Kramer, & S. Madnick (Orgs.), *Data Analytics for Renewable Energy Integration* (Vol. 10097, p. 67–77). Springer International Publishing. https://doi.org/10.1007/978-3-319-50947-1_7

March, J. G., & Shapira, Z. (1987). Managerial Perspectives on Risk and Risk Taking. *Management Science*, *33*(11), 1404–1418. https://doi.org/10.1287/mnsc.33.11.1404

Maxwell, J. A. (2012). *A realist approach for qualitative research*. Sage.

Mihoubi, B., Bouzouia, B., & Gaham, M. (2021). Reactive scheduling approach for solving a realistic flexible job shop scheduling problem. *International Journal of Production Research*, *59*(19), 5790–5808. https://doi.org/10.1080/00207543.2020.1790686

Mikalef, P., Boura, M., Lekakos, G., & Krogstie, J. (2019). Big Data Analytics Capabilities and Innovation: The Mediating Role of Dynamic Capabilities and Moderating Effect of the Environment. *British Journal of Management*, *30*(2), 272–298. https://doi.org/10.1111/1467-8551.12343

Moore, T., Dynes, S., & Chang, F. R. (2015). Identifying how firms manage cybersecurity investment. *Available: Southern Methodist University. Available at: http://blog. smu. edu/research/files/2015/10/SMU-IBM. pdf (Accessed 2022-01-10)*, *32*.

Morse, J. M. (2010). Principles of mixed methods and multimethod research design. In *Sage handbook of mixed methods in social and behavioral research* (p. 189–208). SAGE Publications.

Peteraf, M. A. (1993). The cornerstones of competitive advantage: A resource-based view. *Strategic Management Journal*, *14*(3), 179–191. https://doi.org/10.1002/smj.4250140303

Pigola, A., & da Costa, P. R. (2023). Dynamic Capabilities in Cybersecurity Intelligence: A Meta-Synthesis to Enhance Protection Against Cyber Threats. Communications of the Association for Information Systems, 53(1), 46. Retrieved from https://aisel.aisnet.org/cais/vol53/iss1/46

Posey, C., Raja, U., Crossler, R. E., & Burns, A. J. (2017). Taking stock of organisations' protection of privacy: Categorising and assessing threats to personally identifiable information in the USA. *European Journal of Information Systems*, *26*(6), 585–604. https://doi.org/10.1057/s41303-017-0065-y

Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021). Human Factors in Cybersecurity: A Scoping Review. *The 12th International Conference on Advances in Information Technology*, 1–11. https://doi.org/10.1145/3468784.3468789

Repenning, N. P. (2002). A Simulation-Based Approach to Understanding the Dynamics of Innovation Implementation. *Organization Science*, *13*(2), 109–127. https://doi.org/10.1287/orsc.13.2.109.535

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

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (Eighth edition). Pearson.

Sawyer, B. D., & Hancock, P. A. (2018). Hacking the Human: The Prevalence Paradox in Cybersecurity. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *60*(5), 597–609. https://doi.org/10.1177/0018720818780472

Shamim, S., Zeng, J., Shariq, S. M., & Khan, Z. (2019). Role of big data management in enhancing big data decision-making capability and quality among Chinese firms: A dynamic capabilities view. *Information & Management*, *56*(6), 103135. https://doi.org/10.1016/j.im.2018.12.003

Singh, S. K., & Del Giudice, M. (2019). Big data analytics, dynamic capabilities and firm performance. *Management Decision*, *57*(8), 1729–1733. https://doi.org/10.1108/MD-08-2019-020

Siponen & Vance. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, *34*(3), 487. https://doi.org/10.2307/25750688

Sterman, J. D. (2001). System Dynamics Modeling: Tools for Learning in a Complex World. *California Management Review*, *43*(4), 8–25. https://doi.org/10.2307/41166098

Straub, D. W., & Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, *22*(4), 441. https://doi.org/10.2307/249551

Tashakkori, A., & Teddlie, C. (2010). *Sage handbook of mixed methods in social and behavioral research*. Sage.

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

Tversky, A., & Kahneman, D. (2013). Judgment under Uncertainty: Heuristics and Biases. Em L. C. MacLean & W. T. Ziemba, *World Scientific Handbook in Financial Economics Series* (Vol. 4, p. 261–268). WORLD SCIENTIFIC. https://doi.org/10.1142/9789814417358_0015

van Haastrecht, M., Yigit Ozkan, B., Brinkhuis, M., & Spruit, M. (2021). Respite for SMEs: A Systematic Review of Socio-Technical Cybersecurity Metrics. *Applied Sciences*, *11*(15), 6909. https://doi.org/10.3390/app11156909

Velde, M. van der, Jansen, P., & Anderson, N. (2004). *Guide to management research methods*. Blackwell.

Wamba, S. F., Gunasekaran, A., Akter, S., Ren, S. J., Dubey, R., & Childe, S. J. (2017). Big data analytics and firm performance: Effects of dynamic capabilities. *Journal of Business Research*, *70*, 356–365. https://doi.org/10.1016/j.jbusres.2016.08.009

Wirth, A. (2017). The Economics of Cybersecurity. *Biomedical Instrumentation & Technology*, *51*(s6), 52–59. https://doi.org/10.2345/0899-8205-51.s6.52

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