Analysis of cybersecurity practices in a developing country: The role of firm size and digital strategy

Análisis de prácticas de ciberseguridad en el contexto de un país en desarrollo: El rol del tamaño de empresa y la estrategia digital

Susan Arce*

School of Business, Costa Rica Institute of Technology, Cartago, Costa Rica.

sarce@itcr.ac.cr • https://orcid.org/0000-0001-8978-9623

Mauricio Arroyo

School of Computing Engineering, Costa Rica Institute of Technology Cartago, Costa Rica.

marroyo@itcr.ac.cr • https://orcid.org/0000-0001-6632-4831

Jose Martínez

School of Business, Costa Rica Institute of Technology, Cartago, Costa Rica

jomartinez@itcr.ac.cr • https://orcid.org/0000-0002-7576-4625

• Article received:
30 May, 2025

• Article accepted:
17 November, 2025

• Published online in articles in advance:
22 April, 2026

* Corresponding Author
Susan Arce

DOI:
https://doi.org/10.18845/te.v20i2.8634

Abstract: Digital technologies have revolutionized how firms operate and compete; however, their integration in business processes also amplifies the exposure to cybersecurity threats which might compromise the firm's data integrity and market continuity. Cybersecurity practices have therefore become a priority to secure business operations in the new digitally-led market landscape. This study evaluates the cybersecurity maturity level in Costa Rican firms, distinguishing between SMEs and large firms, aiming to identify shared patterns and challenges faced by these firms in improving their cybersecurity practices. Furthermore, we explore whether adoption of cybersecurity practices is explained by factors related to firm size and the adoption of a formal digital strategy. The results of the cluster analysis on a sample of 66 Costa Rican firms suggest that firms show different levels of cybersecurity maturity, with the most advanced firms consistently excelling at cybersecurity engagement, awareness, and vulnerability management. Also, results reveal that firm size and the presence of a formal digital strategy are strongly associated with cybersecurity maturity: larger firms with a digital strategy tend to be 'cybersecurity leaders', whereas most sampled smaller firms do not have a formal digital strategy and tend to fall into the 'cybersecurity laggards' group, which indicates their greater vulnerability to cyber risks. The identified discrepancies unveil firms' necessity for strategically integrating security considerations into all their processes, and adopt structured, adaptive improvement approaches to mitigate cyber-threats effectively.

Keywords: Cybersecurity, digital strategy, cluster model, cybersecurity awareness, vulnerabilities.

Resumen: Las tecnologías digitales han revolucionado la forma en que las empresas operan y compiten; sin embargo, su integración en los procesos de negocio también amplifica la exposición a amenazas de ciberseguridad que podrían comprometer la integridad de los datos de la empresa y la continuidad del mercado. Por lo tanto, las prácticas de ciberseguridad se han convertido en una prioridad para asegurar las operaciones comerciales en el nuevo panorama del entorno digital. Este estudio evalúa el nivel de madurez en ciberseguridad de las empresas costarricenses, distinguiendo entre pymes y grandes empresas, con el objetivo de identificar patrones

y desafíos compartidos que enfrentan para mejorar su posición en ciberseguridad en medio de los procesos de transformación digital. Además, se explora si la adopción de prácticas de ciberseguridad se explica por factores relacionados con el tamaño de la empresa y la adopción de una estrategia digital formal. Los resultados del análisis de conglomerados en una muestra de 66 empresas costarricenses sugieren que las empresas muestran diferentes niveles de madurez en ciberseguridad, y las más avanzadas sobresalen consistentemente en la participación, la concienciación y la gestión de vulnerabilidades en ciberseguridad. Además, los resultados revelan que el tamaño de la empresa y la existencia de una estrategia digital formal están estrechamente asociados con la madurez en ciberseguridad: las empresas más grandes con una estrategia digital tienden a ser líderes en ciberseguridad, mientras que la mayoría de las empresas más pequeñas de la muestra carecen de una estrategia digital formal y tienden a clasificarse como rezagadas en ciberseguridad, lo que indica su mayor vulnerabilidad a los riesgos cibernéticos. Las discrepancias identificadas revelan la necesidad de las empresas de integrar estratégicamente las consideraciones de seguridad en todos sus procesos y de adoptar enfoques de mejora estructurados y adaptativos para mitigar eficazmente las ciber-amenazas.

Palabras clave: Ciberseguridad, estrategia digital, modelo de conglomerados, conciencia en ciberseguridad, vulnerabilidades.

1. Introduction

In today's business landscape, technological advances have democratized the access to digital technologies, and the digital transformation wave is reshaping industries across the globe (Eller et al., 2020; Acs et al., 2022; Wilson et al., 2023; Lafuente et al., 2024; Vaillant et al., 2025). Organizations, irrespective of their size or sector, are increasingly integrating digital technologies into their operations to improve value-creation and innovation processes, as well as to maintain their competitive position (Verhoef et al., 2021; Clemente-Almendros et al., 2024). This paradigm shift necessitates strategic actions to navigate the complexities of digitalization effectively. Nevertheless, as firms embark on this digital journey, they are exposed to a myriad of cybersecurity threats that can compromise their operations and, ultimately, their survival in the market (OECD, 2024). These challenges are particularly relevant for small and medium-sized enterprises (SMEs) given their well-known resource liabilities (Hoong & Rezania, 2024; Chaudhuri et al., 2025).

Digital technologies have revolutionized traditional business models, enabling firms to streamline processes, access new markets, and deliver augmented solutions to customers (Lafuente & Sallan, 2024; Vaillant & Lafuente, 2024; Rabetino et al., 2025). This digital transformation is not merely a technological upgrade but a fundamental shift in how businesses operate and deliver value. To harness the full potential of digitalization, firms must undertake strategic actions that align with their overall business goals. Such strategies encompass the adoption of appropriate technologies, investment in digital skills, and the reengineering of processes to foster agility and innovation.

The integration of digital technologies also amplifies the exposure to cybersecurity threats. Cyberattacks, data breaches, and other malicious activities have become more sophisticated, posing significant risks to business continuity and data integrity (Neri et al., 2024). Addressing these cybersecurity challenges is imperative, as failure to do so can result in financial losses, market-share damage, and legal repercussions. Therefore, embedding cybersecurity practices within the firm's digital processes is not optional but a critical component of their digital transformation pathway (Li et al., 2022; Wong et al., 2022; Chaudhuri et al., 2025).

Unlike larger firms, SMEs often operate with constrained financial and human resources (Bayon et al., 2016), thus reducing these firms' possibilities for investing in advanced technologies and specialized cybersecurity infrastructure. Additionally, SMEs might lack the expertise to effectively identify and mitigate cyber threats (Hoong & Rezania, 2024). The policy issue pointed out by the OECD (2017, p. 115) carries a clear consideration: "The ability of SMEs to swiftly adopt new

technologies, to learn by doing, innovate, and optimize their production, is constrained by their small scale, limiting their ability to reap the benefits of the digital economy".

This vulnerability is exacerbated by the misconception that SMEs are not prime targets for cyberattacks, leading to complacency in implementing robust cybersecurity measures (Wilson et al., 2023). Consequently, SMEs must adopt specific strategies that balance the pursuit of their market goals with cybersecurity.

In light of these arguments, this study seeks to address the following research questions: To what degree are Costa Rican SMEs adopting cybersecurity practices? Also, do differences exist between small and larger Costa Rican firms when it comes to adopting cybersecurity practices?

To address these questions, the main objective guiding this study is to evaluate the cybersecurity maturity level of Costa Rican firms, distinguishing between SMEs and large firms, aiming to identify shared patterns and challenges faced by these firms when it comes to improving their cybersecurity position amid digital transformation processes.

The empirical exercise uses a unique dataset of 66 Costa Rican firms for 2024. The significance of studying the adoption of cybersecurity practices in the specific context of Costa Rica relies on the country's positioning in technological markets worldwide. The country has emerged as a hub for technology-based international corporations, hosting 12 of the top 30 MedTech original equipment manufacturers (OEMs) and 16 of the top 100 IT companies globally[1]. This influx of multinational tech corporations has created a dynamic ecosystem where local firms have the opportunity to integrate into global value chains and benefit from knowledge spillovers. However, this also places additional pressure on Costa Rican firms to meet international cybersecurity standards to remain competitive and trustworthy partners. Therefore, understanding the configuration of cybersecurity practices adopted by Costa Rican firms is crucial for developing policies and support mechanisms that improve their digital resilience and contribute to the overall stability of the country's digital business park.

The main results suggest large differences in firms' cybersecurity maturity, where a group cybersecurity leaders demonstrates superior levels, in terms of adoption of cybersecurity practices. On contrary, a group of underperforming firms (laggards) shows weak levels of cybersecurity adoption, thus exposing these firms to potential cyber vulnerabilities. Additionally, differences in cybersecurity adoption are strongly linked to firm size and the presence of a digital strategy: larger firms with a digital strategy consistently demonstrate higher adoption levels across all cybersecurity dimensions, whereas most smaller firms do not have a formal digital strategy and tend to show lower cybersecurity maturity, which can leave them more vulnerable to security incidents. The study's emphasis on firm size and digital strategy offers nuanced insights into the heterogeneity of cybersecurity adoption across firm size groups.

The results presented in this research go beyond a mere quantitative exercise, and offer relevant implications. This study contributes to understanding how organizations can effectively match digitalization processes with cybersecurity practices. Prior work has primarily analyzed cybersecurity elements separately (e.g., Li et al., 2019; Hasan et al., 2021; Wong et al., 2022; Heiding et al., 2023; Wilson et al., 2023; Neri et al., 2024), being the study by Chaudhuri et al. (2025) on firms' cybersecurity transformation a welcome exception. But, this mostly fragmented approach overlooks how cybersecurity elements interact to shape firms' cybersecurity maturity. Furthermore, the connection between these practices and firms' strategic choices, in terms of the adoption of a digital strategy, remains underexplored. From a theoretical view, by integrating various cybersecurity elements (i.e., organizational engagement, employees' awareness and training, and vulnerability management) into a unified framework to assess their interplay across different types of firms (in terms of size and adoption of a digital strategy), this study addresses an important gap in the organizational and cybersecurity literature, offering more holistic nuances on cybersecurity adoption in firms operating in a developing context. Therefore, the contribution

1 BBC News: https://www.bbc.com/storyworks/procomer-essential-costa-rica/why-costa-rica-is-becoming-a-prime-destination-for-multinational-companies?utm_source=BBC-ROS&utm_medium=traffic-driver-halfpage&utm_campaign=EssentialCostaRica&utm_content=article1

PR Newswire: https://www.prnewswire.com/news-releases/cinde-costa-rica-launches-new-digital-investor-experience-in-line-with-industry-4-0--301268136.html

of our study lies in showing that cybersecurity maturity is not only a function of technical adoption, but results from the interplay of organizational engagement, employees' awareness and training, and vulnerability management, and that these elements differ systematically with firm size and the adoption of a digital strategy. The empirical analysis demonstrates that technology-centric models to cybersecurity might not present a full picture as to how to effectively introduce cybersecurity practices into business processes. Cybersecurity requires an approach that integrates firms' digitalization processes to upgrading business operations with the adoption of cybersecurity measures (technical practices) to secure technological investments and generate a digitally safe work environment (organizational practices).

The paper is organized as follows. Section 2 presents the background literature, while Section 3 describes the data, variables, and method. Section 4 shows the results of the analysis. The discussion of implications is offered in Section 5, and Section 6 concludes.

2. Related literature

Small and medium-sized enterprises (SMEs) are increasingly reliant on digital technologies to enhance operational efficiency, collaborate with supply chain partners, and reach customers (Eller et al., 2020; Lafuente et al., 2023; Clemente-Almendros et al., 2024). However, SMEs' growing digitalization exposes these firms to cyber risks that can jeopardize business operations, reputational integrity, and financial stability (Hasan et al., 2021; Hasani et al., 2023). Unlike large organizations, SMEs often lack dedicated cybersecurity teams, structured governance, and financial resources, making them particularly vulnerable to cyberattacks (Hoong & Rezania, 2024). The evolving threat landscape and increasing regulatory expectations highlight the need for SMEs to adopt comprehensive cybersecurity practices, not only to mitigate operational risks but also to gain legitimacy with partners and customers (Chaudhuri et al., 2025; Wong et al., 2022). Despite growing awareness, many SMEs struggle with implementation, underscoring the importance of examining the foundational practices that shape their cybersecurity posture.

Based on these arguments, sub-section 2.1 presents the three dimensions of cybersecurity practices analyzed in this study, namely, organizational cybersecurity engagement, cybersecurity awareness and training, and vulnerability to cyber-threats. Together, these three cybersecurity dimensions provide a holistic framework to understand how SMEs organize, operationalize, and respond to cybersecurity challenges. Sub-section 2.2 elaborates on the theoretical arguments linking firm size and digital strategy to the adoption of cybersecurity practices.

2.1 Cybersecurity practices

2.1.1 Organizational cybersecurity engagement

For digitalized firms, the design and implementation of formalized structures, roles, and processes to coordinate cybersecurity at the strategic and operational levels is a key managerial concern. These efforts are often the first step in institutionalizing cybersecurity.

Given the interconnectivity of digital supply chains, firms face increased exposure to external vulnerabilities. A central component of these efforts involves *assigning cybersecurity responsibilities* not only within the organization but also across its broader network of customers, suppliers, and partners. Clearly defined roles for information handling and (physical and digital) asset management among stakeholders help establish mutual accountability and reinforce systemic resilience (Friday et al., 2024). Firms that incorporate such collaborative governance are better positioned to detect and respond to breaches that propagate through partner networks (Li et al., 2019; Hasan et al., 2021).

Establishing an *information security policy* is another key organizational cybersecurity measure. Such policies formalize data protection, users' access, and system maintenance practices, and help building firms' legitimacy by signaling a commitment to cybersecurity not only to internal staff but also to external partners (Chaudhuri et al., 2025). However, many SMEs adopt informal or ad hoc approaches due to limited technical capacity, which can lead to inconsistent implementation of cybersecurity measures (Hoong & Rezania, 2024). Related, SMEs must identify, evaluate, and prioritize risks to allocate scarce resources effectively. *Risk assessment frameworks*—especially those tailored for SMEs, such as Benz and Chatterjee's (2020) cybersecurity evaluation tool—offer practical guidance on gauging exposure to cybersecurity threats. Dynamic and iterative risk assessments help SMEs remain agile as threats evolve, particularly in sectors undergoing rapid digital transformation (Li et al., 2019; Hasan et al., 2021; Chaudhuri et al., 2025).

Finally, *response planning* is an essential but often underdeveloped dimension of organizational cybersecurity efforts. A well-articulated response plan ensures that firms can recover quickly from cyber incidents with minimal operational disruption (Chaudhuri et al., 2025). Involving both internal departments and external actors in designing and testing these plans strengthens communication channels and clarifies escalation protocols (Wong et al., 2022). However, SMEs often struggle to move from basic awareness to action, highlighting the need for simplified templates and management commitment (Hasani et al., 2023).

Overall, efforts towards developing organizational-led cybersecurity measures provide the structural and procedural backbone upon which cybersecurity practices can be built. By engaging stakeholders, codifying expectations, managing risks, and preparing for disruptions, SMEs can create a resilient operational and organizational system.

2.1.2 Cybersecurity awareness and training

While organizational efforts provide structures for cybersecurity, human awareness and competencies determine how effectively these structures function. For SMEs, whose digital defenses often rely on user vigilance, investing in cybersecurity awareness and training is a critical practice that can yield substantial cyber-risk reduction.

Cybersecurity training is a decisive action for enhanced cybersecurity. Unlike larger firms that may have created cybersecurity teams, SMEs depend heavily on general employees to recognize and respond to cyber-threats. Cybersecurity training helps employees to understand the scope of such threats and their responsibilities (James et al., 2013). Research shows that SMEs with consistent training programs report fewer cybersecurity incidents and greater readiness to respond to breaches (Li et al., 2022; Hasani et al., 2023; Friday et al., 2024).

Equally important is the *communication and testing of response and recovery plans*. Awareness alone is insufficient if employees are uncertain about how to act during a cyber incident. SMEs that conduct drills not only improve employees' preparedness but also organizational coordination (Wong et al., 2022). The design of response and recovery plans can also reveal latent weaknesses in internal processes and structures, leading to improved protocols. Testing plans also normalize cybersecurity as part of everyday operations and organizational routines (Chaudhuri et al., 2025).

Integrating cybersecurity functions into human resource practices further strengthens awareness and accountability by embedding cybersecurity into job descriptions, recruitment, performance evaluations, and career development (Hoong & Rezania, 2024). Connecting cybersecurity to internal human resource practices increases the perception that cybersecurity is not the IT department's concern, but rather a priority for the whole organization (James et al., 2013; Hasani et al., 2023). Furthermore, the alignment between human resources and cybersecurity practices supports long-term cultural change (Li et al., 2022; Chaudhuri et al., 2025).

To sum up, cybersecurity awareness and training are indispensable for SMEs navigating digitalization processes. These practices equip employees with the necessary technical and practical knowledge to respond more effectively to cyber-threats.

2.1.3 Vulnerability to cyber-threats

Despite efforts to formalize governance and increase awareness, firms remain vulnerable to a range of cyber-threats. Understanding and managing these vulnerabilities requires continuous monitoring, external intelligence, and rapid assessment capabilities.

The identification and documentation of potential vulnerabilities is the first step to mitigate cyber-threats and their consequences. SMEs often lack comprehensive inventories of IT assets (Eller et al., 2020). Without a clear identification of what needs protection—e.g., software, data repositories, and devices—cybersecurity measures might be misaligned or incomplete (Neri et al., 2024). Systematic asset documentation enables SMEs to assess the potential impact of threats and to prioritize mitigation efforts accordingly (Hasan et al., 2021).

Given their resource limitations, SMEs increasingly rely on external sources for threat and vulnerability information. Governmental alerts, sector-specific advisories, cybersecurity associations, and vendor-provided intelligence can serve as critical inputs for anticipating new threats (Benz & Chatterjee, 2020). Nevertheless, as Hoong and Rezania (2024) emphasized, the value of external information largely depends on SMEs' capacity to contextualize technical data (interpretation) and generate actionable strategies to react timely to cyber-threats. *Timely identification and assessment of potential threats* is therefore essential for minimizing the consequences of cyber-threats. Many SMEs still rely on informal methods, such as employee intuition or reactive troubleshooting, to detect cyber incidents (James et al., 2013). More structured approaches—e.g., automated monitoring, anomaly detection systems, or employee-reported suspicious behavior—can enable earlier intervention (Li et al., 2022).

What differentiates more resilient SMEs is their ability to *integrate technical indicators with business decision-making*. This action involves translating cyber-threat information into business language, facilitating decision-makers to weigh trade-offs and react to cyber incidents (Hasani et al., 2023). Chaudhuri et al. (2025) underscored that the integration of technical and strategic perspectives is a strong sign of mature cybersecurity practices, even in resource-constrained environments.

Ultimately, managing vulnerability to cyber-threats is not about eliminating all cyber-risks, but about developing structures to better detect, evaluate, and respond to cyber-threats rapidly, thus creating a safer organizational environment. For SMEs, whose survival may hinge on a single cyber incident, such capacities are needed to secure their operations and performance in the long-run.

2.2 The role of firm size and digital strategy in cybersecurity adoption

This study views firm size and digital strategy as organizational enablers that condition the adoption of cybersecurity practices across the three dimensions discussed in Section 2.1—organizational engagement, awareness/training, and vulnerability management. From an organization and management perspective (Bharadwaj et al., 2013; Tam et al., 2021), the integration of cybersecurity into everyday operations depends on how firms organize and align resources and routines around digital transformation priorities (Verhoef et al., 2021).

Concerning firm size, a consistent pattern reported in prior work is that cybersecurity maturity tends to increase with size, reflecting deeper resource endowments, access to specialized personnel, and stronger exposure to compliance pressures and supply-chain requirements (Hasan et al., 2021; Tam et al., 2021; Neri et al., 2024). Also, Dinkova et al. (2024) showed that SMEs invest less in cybersecurity than large businesses; however, SMEs do not report more cyber incidents, thus suggesting that these firms are not more vulnerable than their larger counterparts, which are usual targets of cyber-attacks (Hoong & Rezania, 2024). Translating this evidence to the adoption of cybersecurity practices, larger firms typically have greater financial resources, which enable them to invest in advanced technologies, systematize vulnerability assessment and testing, and dedicate resources to targeted training and cybersecurity teams (Friday et al., 2024; Chaudhuri et al., 2025).

By contrast, SMEs face resource and capability constraints (OECD, 2017; Eller et al., 2020; Clemente-Almendros et al., 2024) and sometimes attitudinal underestimation of cyber risks (Wilson et al., 2023), which can dilute the effects of any effort directed towards improving the firm's cybersecurity. But, it has also been found that SMEs can progress markedly when they leverage standardized frameworks and external guidance (Benz & Chatterjee, 2020), embed basic governance, and connect training to role clarity (James et al., 2013; Vroom & Von Solms, 2004).

From this body of literature it can be deduced that firm size influences technical investments and program implementation, as well as the organizational structures that govern cybersecurity plans and measures. Therefore, the following hypothesis is proposed:

H1: Firm size, in terms of employees, is positively correlated with the adoption of cybersecurity practices.

Besides firm size, a clearly articulated digital strategy operates as a managerial mechanism that allows firms to align cybersecurity with digitalization goals which, in turn, reduces coordination problems and fragmentation in decision-making, while facilitating the development of 'cybersecurity-by-design' actions and technology choices (Bharadwaj et al., 2013; Verhoef et al., 2021). Recent work underscores that cybersecurity maturity reflects not only technical controls, but also managerial choices about awareness, governance, and intra- and inter-firm coordination (Wong et al., 2022; Hoong & Rezania, 2024; Chaudhuri et al., 2025).

Firms with a digital strategy are in a better position to formalize information security policies and roles (Li et al., 2019) and invest in tailor-made training programs and response/recovery plans (Hasani et al., 2023; Wong et al., 2022), and incorporate vulnerability information into risk-based decision-making (Neri et al., 2024; Heiding et al., 2023). Implementation time also matters: longer-lived strategies typically enable cumulative learning and routinization, which support higher cybersecurity maturity (Hasan et al., 2021; Li et al., 2022). On contrary, without a formal digital strategy firms' cybersecurity will likely rely on tool-centric spending and weak protocols that lack the structured organizational support needed to translate cyber-controls into reliable routines (Vroom & Von Solms, 2004; Neri et al., 2024; OECD, 2024).

Therefore, a digital strategy acts as a strategic glue, a capability that helps to align human capabilities, technological tools, and organizational processes in a coherent cybersecurity framework, which facilitates the shift from treating cybersecurity as a purely technical safeguard to managing it as a strategic asset that supports competitive advantage (Porter & Heppelmann, 2014; Teece, 2018). Based on this body of literature we hypothesize:

H2: Firms with a formal digital strategy will demonstrate greater cybersecurity maturity.

3. Data, variable, and method

3.1 Data

The data used for this study is based on a survey on digitalization and cyber risks. The survey characterizes the companies' use of different digital tools and the cybersecurity level for each firm according to the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF). The data was collected through an online structured questionnaire using LimeSurvey. The unit of analysis is the business, and the instrument was answered by the General Manager (CEO) or the person responsible for the company's information and communications technology (ICT).

Data was collected between September and November 2024. After removing observations with incomplete data, the final clean sample used for this study consists of 66 companies. The diversity of economic activity corroborates the validity of the final sample. Table 1 shows the breakdown by industry: manufacturing (20%), retail (43%), knowledge-intensive business services (KIBS) (17%), and other (agro-food and consumer-oriented services) (20%).

Additionally, a further inspection of the data reveals that SMEs—with less than 250 employees—represent 69.70% of the sampled firms (46 observations). Concerning the economic activity of the two sub-samples, a similar industry distribution was found: manufacturing SMEs= 20% (20% for large firms), SMEs in retail sectors= 48% (30% for large firms), KIBS SMEs= 15% (20% for large firms), and SMEs in other industries (agro-food and consumer-oriented services)= 17% (30% for large firms). The reported similarity in industry distribution across size categories suggests that the industry composition is unlikely to bias the comparison of cybersecurity practices between SMEs and large firms.

3.2 Variables

3.2.1 Cybersecurity practices

In this subsection, we describe the variables dealing with the adoption of the studied cybersecurity dimensions: organizational cybersecurity engagement, cybersecurity awareness and training, and vulnerability to cyber-threats. Respondents were asked along a five-point Likert scale to value the individual importance of the analyzed cybersecurity practices, and such items are only valuable if deemed so by the respondent (Benz & Chatterjee, 2020).

In the Likert-type scale, a value of one designates low relevant variables, that is, the focal cybersecurity practice is not formalized, is incomplete or in progress; a value of two indicates a formalization level (the focal practice is defined or approved but not yet implemented); a value of three refers to formally implemented practices that are part of operational processes and; finally, a value of four indicates that the focal cybersecurity practice is fully aligned with industry standards or best practices. The rate of zero indicates that the focal cybersecurity practice has no strategic value whatsoever, and the remaining scale points ensure the uniform assessment of the analyzed practices' importance. Notice that the division of the positive scale values (from 1 to 4) allows a sufficient degree of differentiation in the analysis of the studied cybersecurity practices (Lederer et al., 2013).

Prior studies have used similar scales to evaluate different problems related to strategic planning (Lederer et al., 2013), as well as the analysis of business competitiveness (Lafuente et al., 2020) and entrepreneurial ecosystems (Lafuente et al., 2021).

Organizational cybersecurity engagement.—According to Li et al. (2022), organizational engagement include actions to fight cybersecurity crime as an antecedent of threat and coping appraisals. Organizational engagement was measured by the cybersecurity roles and responsibilities established (customers, suppliers, and partners) in asset management (Hasan et al., 2021); the establishment of an information security policy (Herath and Rao, 2009); whether information security roles and responsibilities are defined (Herath & Rao, 2009); as well as the establishment of risk management processes and response plans (incident response and business continuity) (Hasan et al., 2021).

Cybersecurity awareness and training.—For the purpose of this paper, cybersecurity awareness is understood as the knowledge of vulnerabilities, threats and mitigation to protect the enterprise's information and systems (Chaudhary et al., 2022), specifically the tactics and targets employed by cybercriminals, how to recognize possible dangers, and actions to prevent being victims of these attacks, while cybersecurity training refers to enabling employees with the latest security practices to proactively identify and address potential cyber threats (Chaudhuri et al., 2025).

Respondents were asked to evaluate their cybersecurity awareness level on a set of specific items to determine whether all users are informed and trained on security-related responsibilities (Chaudhuri et al., 2025); if the company tests response and recovery plans (Hasan et al., 2021; Tam et al., 2021); and whether cybersecurity functions are included in

human resources practices (both in training and recruitment) (Vroom & Von Solms, 2004). Finally, regarding response and recovery actions, they were measured by asking managers to mention if their staff is aware of their roles and order of operation when a response is necessary, and if recovery activities are communicated to internal stakeholders, executives, and the management team (Hasan et al., 2021).

Vulnerability to cyber-threats.—Vulnerability analysis or assessments regarding cyber-threats refer to weaknesses in a system or its design that allow an intruder to execute commands, access unauthorized data, and/or conduct denial-of-service (Abomhara & Køien, 2015). Specific items were included in the survey instrument to identify asset vulnerabilities (Heiding et al., 2023); threat and vulnerability information received from shared sources (Chaudhuri et al., 2025); the assessment of internal or external threats as they arise (Hasan et al., 2021); as well as the identification of potential threats, vulnerabilities, probabilities, and business impacts to determine risk (Heiding et al., 2023). Finally, respondents were asked if their companies performed vulnerability tests regularly (Hasan et al., 2021).

3.2.2 Profile variables

A set of variables linked to the firms' profile was included to analyze the role of scale and digital strategy on the adoption of cybersecurity practices, namely, firm size, age, digital strategy, and economic activity. The number of employees measures firm size, and firm age is determined by the number of years of market experience. Both firm size and firm age were logged to reduce skewness.

Digital strategy is defined as an organizational strategy that employs digital resources to create differential value (Bharadwaj et al., 2013; Mora-Esquivel & Leiva, 2025). In the questionnaire, respondents were asked as to whether the firm has adopted a formal digital strategy, that is, an organizational scheme to managing and implementing digital technologies and digitization processes at all business levels. Additionally, for adopting firms, managers indicated the implementation year of the firm's digital strategy. From these responses, a dummy variable was created to identify the group of firms that have adopted a digital strategy, while a count variable was used to account for the number of years since the digital strategy was implemented. Descriptive statistics presented in Table 1 show that 62% of the companies have adopted a digital strategy, and the average number of years since it was implemented is 6.91 years.

Finally, a set of industry dummy variables were included to record firms' economic activity according to the NACE codes: manufacturing, retail, knowledge-intensive business services (KIBS), and other activities (agro-food and consumer-oriented services).

3.3 Method

The empirical strategy adopted to test the study's hypotheses is based on two complementary methods.

In the first stage, we employ a non-hierarchical cluster model (K-means) to evaluate firms' cybersecurity practices, using the variables in Panels A-C of Table 1 as inputs.

The non-hierarchical cluster analysis is based on the Euclidean distance between vectors of the standardized values of the studied variables (Anderberg, 1973; Everitt, 1980). Through this procedure observations—in our case, firms—are classified according to the similarities in the analyzed cybersecurity dimensions. The K-means cluster requires the establishment of a fixed number of clusters, which represents the main pitfall of this model because in many research fields (including social sciences) cluster analyses are often exploratory.

To corroborate the number of clusters and the validity of the proposed analysis, we used the Calinski and Harabasz (1974) statistic. This index is obtained as $\mathrm{CH}\left(\mathrm{k}\right) = \frac{\frac{\mathrm{B(k)}}{(\mathrm{k}-1)}}{\frac{\mathrm{W(k)}}{\mathrm{n}-\mathrm{k}}}$, where *B(k)* and *W(k)* are the between- and within-cluster sums of squares, with *k* clusters, respectively. Since *B(k)* > *W(k)*, the largest *CH(k)* value indicates the best clustering. In this study, the number of clusters that maximizes the *CH(k)* index is 3 (pseudo-F value: 41.94). Therefore, the final non-hierarchical cluster asks for a three-way division. The full set of results of the *CH(k)* statistic computed in this study is presented in Appendix 1.

Table 1: Descriptive statistics for the study's variables (sample size: 66 firms)

Variable	Average	Std. dev.	Q1	Q3
Panel A: Organizational cybersecurity engagement				
Cybersecurity roles and responsibilities established (customers, suppliers, and partners) in asset management	2.65	1.45	2	4
Information security policy established	2.82	1.36	2	4
Information security roles and responsibilities are defined	2.71	1.34	2	4
Risk management processes are established	2.64	1.45	2	4
Response plans (incident response and business continuity) are in place and managed	2.52	1.46	2	4
Panel B: Cybersecurity awareness and training				
All users are informed and trained on security-related responsibilities	2.68	1.46	2	4
Response and recovery plans are tested	2.61	1.53	1	4
Cybersecurity functions are included in human resources practices (in training and recruitment)	2.03	1.66	0	4
Staff is aware of their roles and order of operation when a response is necessary	2.82	1.40	2	4
Recovery activities are communicated to internal stakeholders, executives, and the management team	2.55	1.45	1	4
Panel C: Vulnerability to cyber-threats				
Asset vulnerabilities are identified and documented	2.61	1.49	1	4
Threat and vulnerability information is received from forums and shared sources	2.23	1.63	0	4
Internal or external threats are assessed as they arise	2.89	1.27	2	4
Potential threats, vulnerabilities, probabilities, and business impacts are identified to determine risk	2.79	1.42	2	4
Vulnerability tests are performed regularly	2.21	1.65	0	4
Panel D: Firms' profile				
Firm size (employees)	378.11	900.78	17	300
Firm age (years)	30.73	24.23	11	46
Digital strategy: adoption (dummy)	0.62	0.49	0	1
Digital strategy: implementation time (years)	6.91	8.41	0	10
Manufacturing	0.20	0.40	0	0
Retail	0.43	0.50	0	1
Knowledge-intensive business services (KIBS)	0.17	0.38	0	0
Other (agro-food and consumer-oriented services)	0.20	0.31	0	0

In the second stage, an ordered logit model is estimated to analyze the determinants of a firm's position within the cybersecurity maturity spectrum. In this model, the dependent variable is the ordinal cluster membership computed in the first stage (cybersecurity maturity levels: 'leaders'= 1, 'developers'= 2, and 'laggards'= 3). The independent variables include firm size (ln employees), a dummy variable accounting for the adoption of a digital strategy, implementation time of the digital strategy (ln years), and industry as control variable (agro-food and consumer-oriented services is the omitted industry category).

Given that the categories of cybersecurity maturity follow a hierarchical structure (i.e., an ordered discrete variable), the ordered logit model was chosen as econometric technique to formally test the study's hypotheses (Long, 1997).

The ordered logit model is an extension of the standard logistic regression applied when the dependent variable is categorical and has a meaningful order with more than two categories (Long, 1997; Greene, 2003). The ordinal

logit model is estimated via maximum likelihood and can be expressed in terms of the probability of revealing a given cybersecurity maturity level as:

$$\Pr\left(y_i > j\right) = \frac{\exp(X_i\beta - \varphi_j)}{1+\exp(X_i\beta - \varphi_j)}, \quad j = 1, 2, 3 \qquad (1)$$

where *j* is cybersecurity maturity level, *Xi* is the vector of independent variables, β is the vector of coefficients to be estimated that vary across the categories of the dependent variable, and ϕ_j are cut-off points for the thresholds of the ordered model.

This approach provides a robust statistical test of whether firm size and the adoption of a digital strategy influence firms' cybersecurity maturity level, thereby directly addressing the second research question and reinforcing the theoretical link between organizational characteristics and cybersecurity adoption.

As for the study's hypotheses, we expect a positive result for the coefficients linked to firm size and digital strategy to confirm that size (in terms of employees) (H1) and the adoption of a digital strategy (H2) are positively correlated with the adoption of cybersecurity practices.

4. Results

4.1 Cluster analysis: Identifying the level of cybersecurity maturity

This section presents the results of the cluster analysis aimed at identifying patterns of cybersecurity practices adopted by the analyzed Costa Rican firms. The cluster model yielded three clearly differentiated groups of firms based on their levels of cybersecurity practices: 'cybersecurity leaders', 'cybersecurity developers', and 'cybersecurity laggards'. These groups demonstrate marked differences in terms of their profile as well as the cyber-security practices evaluated (organizational cybersecurity engagement, awareness and training, vulnerability management). For each group, Table 2 shows the results for the profile variables while the main findings for the cybersecurity variables analyzed in this study are presented in Table 3.

The first group (n= 20), cybersecurity leaders, includes the most mature firms in terms of cybersecurity practices. These firms are, on average, the largest (673.75 employees) and oldest (42.05 years) in the sample, with 70% having adopted a digital strategy and an average time since implementation of 8.95 years, which can be interpreted as evidence of advanced digital maturity. Finally, this group includes the largest proportion of firms in knowledge-intensive business services (KIBS) activities (25%), thus suggesting a high alignment between their operational processes and cybersecurity practices (technology-strategy fit) (Table 2).

The findings in Table 3 indicate that this group shows the highest levels for the three analyzed cybersecurity dimensions. The results highlight the high *organizational cybersecurity engagement* among these firms (the variables with the highest scores are 'response plans', 'definition of information security roles and responsibilities', and 'cybersecurity roles and responsibilities in asset management'). These findings, in particular for the cybersecurity of asset management processes and response plans, are in line with prior work emphasizing the relevance of institutionalizing cybersecurity practices if the development of measures that safeguard business operations is the desired goal (e.g., Hasani et al., 2023; Friday et al., 2024).

In terms of *cybersecurity awareness and training*, these firms score uniformly high, with the exception of the variable linked to the 'definition of cybersecurity functions in human resources practices. This result reflects the strategic integration of technical and human dimensions of cybersecurity within firm operations (Wong et al., 2022). Among these firms, the approach to *vulnerability management* is also advanced, especially for the variables linked to the identification and

assessment of cyber-threats ('Internal or external threats are assessed as they arise' and 'Potential threats, vulnerabilities, probabilities, and business impacts are identified to determine risk'). This implies that, in this group, cyber-risks are evaluated not just technically but also in terms of their potential operational and economic impact, which might contribute to firms' cyber-resilience (Neri et al., 2024).

Table 2: Profile of firms included in the groups emerging from the cluster model

	Group 1 (Leaders)	Group 2 (Developers)	Group 3 (Laggards)
Firm size (employees)	673.75 (1388.53)	335.32 (647.75)	72.33 (149.96)***
Firm age (years)	42.05 (25.94)	28.26 (24.24)**	20.73 (15.81)***
Digital strategy: adoption (dummy)	0.70 (0.47)	0.71 (0.46)	0.33 (0.49)**
Digital strategy: implementation time (years)	8.95 (9.79)	6.77 (7.33)	4.47 (8.39)*
Manufacturing	0.25 (0.44)	0.13 (0.34)*	0.27 (0.46)
Retail	0.35 (0.49)	0.48 (0.51)	0.40 (0.51)
Knowledge-intensive business services (KIBS)	0.25 (0.44)	0.13 (0.34)*	0.13 (0.35)*
Other (agro-food and consumer-oriented services)	0.15 (0.25)	0.25 (0.28)	0.20 (0.28)
Observations	20	31	15

*Standard deviation is presented in parentheses. *, **, *** = significant at the 10%, 5%, and 1%, respectively. For the three cluster columns, the test compares the results between Group 1 and Group 2 and between Group 1 and Group 3 (Mann-Whitney U test).*

The second group—cybersecurity developers—consists of 31 firms, with an average size of 335.32 employees and an average age of 28.26 years. Although for these firms digital strategy adoption is similar to that reported for Group 1 (71%), their implementation duration is shorter (6.77 years) (Table 2). These firms, mostly operating in retail and consumer-oriented services, demonstrate moderate cybersecurity maturity, reflecting ongoing development efforts.

Notice that in this group 'information security policies' and 'risk management processes' are the most important *organizational cybersecurity engagement* practices (Table 3). On contrary, 'defined cybersecurity roles and responsibilities' and 'response plans' are areas that need improvement. To sum up, these firms seem to be carrying out efforts towards the creation of structured cybersecurity governance (Chaudhuri et al., 2025; Hoong & Rezania, 2024).

Cybersecurity awareness and training efforts are unevenly distributed in this group. While response plans and staff role clarity are well structured in this group ('response and recovery plans are tested' and 'staff is aware of their roles and order of operation when a response is necessary'), employees' training and inclusion of cybersecurity functions in human resource practices are less consistent. These results suggest that awareness is a strategic concern in this group, but there is insufficient organizational support to drive behavioral change across the organization (Li et al., 2022). Their *vulnerability to cyber-threats practices* reflects a partial position. Whereas the identification of potential cyber vulnerabilities and their impact on the business is well identified, vulnerability testing is inconsistent, which might indicate that these firms acknowledge the value of recognizing cyber-risks, but the operationalization of protection strategies is not fully developed (Benz & Chatterjee, 2020) (Table 3).

The 15 firms included in the third group (cybersecurity laggards) are the smallest (72.33 employees) and youngest (20.73 years) in the sample. Also, these firms are in the early stage of the digital transformation process: only 33% have adopted a digital strategy, and the average implementation time is the lowest among the sampled firms (4.47 years) (Table 2).

Firms in this group consistently underperform in all the analyzed cybersecurity dimensions, signaling high vulnerability and low organizational readiness. In the case of the *organizational cybersecurity engagement* practices, firms in this group show extremely low levels of formalized practices and underdeveloped response planning. These results highlight structural weaknesses and echo concerns about the gaps in digitalization and cyber readiness among small, resource-constrained firms stressed in prior research (Lafuente et al., 2019; Benz & Chatterjee, 2020; Friday et al., 2024).

Concerning *cybersecurity awareness and training*, this group shows a poor integration of cybersecurity into human resource practices, while staff roles in cyber-incident response are poorly defined. This group lacks both a cybersecurity culture and investments in employee-centered cybersecurity (Wong et al., 2022). Finally, for the practices related to *vulnerability to cyber-threats*, results reveal that these firms are highly exposed to cyber incidents. The identification and documentation of cyber vulnerabilities, evaluation of the impacts of cyber-risks, and vulnerability testing are the weakest points in this group (Table 3). The lack of systematic threat identification and assessment leaves firms in this group particularly vulnerable to disruption (Hasan et al., 2021; Neri et al., 2024).

Table 3: Cluster analysis: Results

	Group 1 (Leaders)	Group 2 (Developers)	Group 3 (Laggards)
Panel A: Organizational cybersecurity engagement			
Cybersecurity roles and responsibilities established (customers, suppliers, and partners) in asset management	3.90 (0.31)	2.68 (1.05)***	0.93 (1.39)***
Information security policy established	3.85 (0.37)	3.00 (0.97)***	1.07 (1.22)***
Information security roles and responsibilities are defined	3.95 (0.22)	2.74 (1.00)***	1.00 (0.93)***
Risk management processes are established	3.65 (0.93)	2.97 (0.84)***	0.60 (0.99)***
Response plans (incident response and business continuity) are in place and managed	3.95 (0.22)	2.61 (0.84)***	0.40 (0.74)***
Panel B: Cybersecurity awareness and training			
All users are informed and trained on security-related responsibilities	3.85 (0.49)	2.55 (1.31)***	1.40 (1.45)***
Response and recovery plans are tested	3.85 (0.37)	2.81 (1.11)***	0.53 (1.06)***
Cybersecurity functions are included in human resources practices (in training and recruitment)	3.55 (0.94)	1.94 (1.46)***	0.20 (0.41)***
Staff is aware of their roles and order of operation when a response is necessary	3.80 (0.41)	2.97 (1.08)***	1.20 (1.47)***
Recovery activities are communicated to internal stakeholders, executives, and the management team	3.80 (0.41)	2.39 (1.23)***	1.20 (1.42)***
Panel C: Vulnerability to cyber-threats			
Asset vulnerabilities are identified and documented	3.85 (0.49)	2.81 (1.05)***	0.53 (0.83)***
Threat and vulnerability information is received from forums and shared sources	3.35 (1.46)	2.48 (1.18)***	0.20 (0.41)***
Internal or external threats are assessed as they arise	4.00 (0.00)	2.84 (0.78)***	1.53 (1.55)***
Potential threats, vulnerabilities, probabilities, and business impacts are identified to determine risk	3.90 (0.31)	3.03 (0.91)***	0.80 (1.15)***
Vulnerability tests are performed regularly	3.55 (1.23)	2.39 (1.17)***	0.07 (0.26)***
Observations	20	31	15

*Standard deviation is presented in parentheses. *, **, *** = significant at the 10%, 5%, and 1%, respectively. For the three cluster columns, the test compares the results between Group 1 and Group 2 and between Group 1 and Group 3 (Mann-Whitney U test).*

4.2 Ordered logit model: Hypotheses testing

To further investigate the role of firm size and digital strategy in explaining differences in cybersecurity maturity, we estimated an ordered logit regression using the ordinal cluster membership variable estimated from the first stage analysis as the dependent variable. Regression results and average marginal effects are presented in Table 4.

Prior to presenting the results, notice that the variance inflation factor (VIF) was computed to test whether coefficients are amplified due to correlations across the explanatory variables. The average VIF value for the full model in Table 4 is 2.36 (range = 1.55-4.19). The results of this diagnostic test suggest that the model specification does not suffer from collinearity problems, thus further validating our empirical approach (Greene, 2003).

The results show that firm size is positively and significantly associated with higher cybersecurity maturity: large firms are more likely to belong to the 'leaders' cluster, compared to SMEs, holding other factors constant. In terms of interpretation, notice that because size enters as a logged term in the model, proportional size changes translate linearly into probability changes. The result of the marginal effect for the variable size indicates that, holding other variables constant, a 50% increase in firm size (e.g., from 10 to 15 employees) rises the probability of being a cybersecurity 'leader' by 2.03 percentage points (). This significant result, together with the finding obtained for the 'laggard' group, leads to confirm our first hypothesis (H1) stating that firm size, in terms of employees, is positively correlated with the adoption of cybersecurity practices.

In the case of the digital strategy, the findings indicate that this variable has a positive effect on cybersecurity maturity level. Specifically, the results for the marginal effects in Table 4 suggest that the probability of being a cybersecurity 'leader' increases 27 percentage points for firms with a formal digital strategy, relative to the probability of firms that do not have a digital strategy. This finding reinforces the theoretical expectation that firms' strategic orientation (in terms of digital strategy) is a critical enabler of cybersecurity adoption, and confirms our hypothesis H2 which states that firms with a formal digital strategy will demonstrate greater cybersecurity maturity.

To sum up, by integrating the results of the cluster analysis with the ordered logit regression, we provide both an exploratory classification of firms' cybersecurity maturity levels and an analysis of how factors related to firms' structural capacity (size) and strategic orientation (digital strategy) influence firms' cybersecurity maturity levels.

Table 4: Ordered logit model: Regression results

		Average marginal effects (std. error)		
	Coefficients (std. error)	**Group 1 (Leaders)**	**Group 2 (Developers)**	**Group 3 (Laggards)**
Firm size (employees)	–0.28 (0.15)*	0.05 (0.02)**	–0.01 (0.01)	–0.04 (0.02)*
Digital strategy: adoption (dummy)	–1.50 (0.90)*	0.27 (0.15)*	–0.05 (0.05)	–0.22 (0.14)
Digital strategy: implementation time (years)	0.33 (0.36)	– 0.06 (0.06)	0.01 (0.01)	0.04 (0.05)
Firm age (years)	–0.60 (0.33)*	0.11 (0.06)*	–0.02 (0.02)	–0.09 (0.05)*
Industry dummies	Yes			
Cut 1	–5.43 (1.02)***			
Cut 2	–2.90 (0.98)***			
Log pseudolikelihood	–61.14			
Wald test (chi2)	24.26***			
Pseudo R2	0.1207			
VIF (min-max)	2.36 (1.55-4.19)			
Observations	66	20	31	15

*Robust standard error is presented in parentheses. Agro-food and consumer-oriented services is the omitted industry category. *, **, *** = significant at the 10%, 5%, and 1%, respectively.*

5. Discussion of implications

5.1 Discussion

This study set out to examine how firm size and the adoption of a digital strategy influence the maturity of cybersecurity practices in Costa Rican SMEs and large firms. Guided by postulates from the strategic management literature and the capability perspective (Bharadwaj et al., 2013; Teece, 2018), our objective was to move beyond a purely technical framing of cybersecurity and assess how factors linked to firms' structural capacity (size) and strategic orientation (digital strategy) shape the adoption of cybersecurity practices. By combining an exploratory cluster model with an ordered logit model, we provide an integrated view of both the configuration of cybersecurity practices and the organizational determinants that underlie the reported patterns.

The analysis underscores the importance of a bundled, cross-dimensional approach to cybersecurity adoption. The three identified clusters—i.e., leaders, developers, and laggards—reveal that advanced cybersecurity maturity is not the product of isolated initiatives, but rather the coordinated deployment of organizational resources, the coordination of processes, employee awareness, and systematic vulnerability management (Hasan et al., 2021; Chaudhuri et al., 2025; Friday et al., 2024). This aligns with prior work emphasizing that organizational enablers condition the routinization of cybersecurity practices through the alignment of resources, processes, and managerial priorities (Bharadwaj et al., 2013; Verhoef et al., 2021).

Specifically, firm size emerges as a consistent factor that explains cybersecurity maturity, reflecting the logic that larger organizations possess greater capacity to invest in specialized personnel, monitoring tools, and formalized governance (Hasan et al., 2021; Tam et al., 2021; Neri et al., 2024). Yet the findings also challenge deterministic interpretations: some SMEs attain high maturity when a digital strategy is in place, suggesting that strategic orientation can compensate for resource limitations by providing strategic guidance and prioritization mechanisms (Wong et al., 2022). This interplay between size and strategy orientation, which we link to a relevant capability, highlight the importance of resource orchestration configure cybersecurity practices (Porter & Heppelmann, 2014).

Digital transformation is a process that requires significant efforts at all firm levels (Lafuente et al., 2018; Rojas-Segura et al., 2023; Escribá-Carda et al., 2024). The strong effect of adopting a formal digital strategy reinforces its role as a central managerial capability to organize assets (tangible and intangible) and coordinate internal processes (Mora-Esquivel and Leiva, 2025). Firms with such strategies are more likely to embed cybersecurity into broader digital transformation efforts (Verhoef et al., 2021; Chaudhuri et al., 2025) that, in turn, help to institutionalize cybersecurity practices that will likely be reinforced over time (Hasani et al., 2023; Li et al., 2019). The integration of cybersecurity within a firm's strategic architecture facilitates cyber-policy codification, role assignment, and the development of training programs that advance cyber-maturity (Hoong & Rezania, 2024; Wong et al., 2022). This is in line with recent work emphasizing that digital strategies serve as roadmaps for technology adoption, as well as governance mechanisms that align human, technical, and procedural elements in support of sustained performance (Bharadwaj et al., 2013; Porter & Heppelmann, 2014).

Taken together, the results presented in this study contribute to strategic management research by linking observable maturity patterns to underlying organizational enablers. They show that building robust cybersecurity practices is much more than a mere technological investment, but implies the alignment of the firm's strategic goals with operational execution in ways that reinforce intra-firm complementarities (Bharadwaj et al., 2013; Melville et al., 2004). This helps explain why fragmented, tool-centric approaches often fail to deliver effective cybersecurity plans, whereas integrated strategies boost firms along the maturity trajectory from low to high levels of cybersecurity maturity (Hasan et al., 2021; Chaudhuri et al., 2025; Friday et al., 2024).

5.2 Implications for academia

The results presented in this study have important implications for academia and practice. For cybersecurity research, prior work has called for more granular examinations of how organizational characteristics influence cybersecurity behaviors (Hasan et al., 2021; Hasani et al., 2023). Our identification of three distinct clusters—leaders, developers, and laggards—provides a refined framework that explains how cybersecurity practices co-evolve with organizational development and digital maturity. The resulting typology also supports the theoretical claim that the adoption of cybersecurity practices is not a path-dependent process shaped by strategic intent, resource availability, and organizational commitment (Chaudhuri et al., 2025; Hoong & Rezania, 2024). Related, this study advances an empirical typology of cybersecurity implementation within firms operating in a developing economy. Future work can build on these results to develop more holistic models that account for cross-dimensional enablers and inhibitors of cybersecurity adoption, especially in under-researched contexts.

Second, the study enriches the literature on socio-technical perspectives of cybersecurity by showing how human, organizational, and technological practices interact in shaping firm-level cybersecurity postures. The reported variations across cybersecurity awareness and training practices, especially the integration of cybersecurity into human resource processes, illustrate that technology-centric models might be insufficient to explain the effective integration of cybersecurity practices into business operations. These findings align with the growing body of research emphasizing managerial and governance dimensions of cybersecurity (Wong et al., 2022; James et al., 2013).

5.3 Implications for practitioners

For managers, the findings presented in this study provide a practical roadmap for benchmarking cybersecurity policies. The differentiation between cybersecurity leaders, developers, and laggards offers the opportunity for firms to self-assess their cybersecurity position and identify concrete gaps in their practices. For example, managers of firms catalogued as cybersecurity laggards will be well advised to prioritize investments in key areas, such as information security policies and vulnerability identification and response planning, while firms in the cybersecurity developers group might benefit from developing cybersecurity awareness programs and vulnerability testing. Related, a step-wise process to cybersecurity might enable resource-constrained firms to progress incrementally in their cybersecurity maturity based on their capabilities and specific needs.

Second, the results highlight the importance of embedding cybersecurity into broader digital transformation strategies. The group of cybersecurity leaders is characterized by having a more consolidated digital strategy, which suggests that cybersecurity implementation is a strategic process that should match technical issues with organizational processes. As digital technologies are increasingly integrated into operations, firms must treat cybersecurity as a key business function. Industry chambers can use these insights to develop tailored support programs and training initiatives that facilitate structured cybersecurity developments across firms operating in different sectors. Promoting inter-firm collaboration and knowledge-sharing, especially in sectors with limited digital maturity, could also accelerate cybersecurity-capability building at the territorial level (Lafuente et al., 2022).

6. Concluding remarks and future research

6.1 Conclusion

This study investigated the cybersecurity maturity level of Costa Rican firms, focusing on shared patterns and challenges in the context of ongoing digital transformation processes. Through a cluster analysis, we identified three distinct groups of firms, in terms of the adoption of cybersecurity practices: leaders, developers, and laggards. These groups show marked discrepancies in their cybersecurity maturity across three analyzed dimensions of cyber-practices (organizational cybersecurity engagement, cybersecurity awareness and training, and vulnerability to cyber-threats).

The findings reveal that a small proportion of firms demonstrate high cybersecurity maturity, while the majority are either in the process of developing practices or remain significantly underprepared. Firms in the cybersecurity leaders group show a comprehensive, institutionalized approach to cybersecurity, whereas cybersecurity developers show partial engagement and inconsistencies, and laggards lack foundational cybersecurity structures. These findings highlight both the uneven implementation of cybersecurity practices among Costa Rican firms and the presence of critical gaps that might hinder secure digitalization processes.

6.2 Future research

This study opens various avenues for future research. First, future work should take a longitudinal approach to analyze how firms transition towards high cybersecurity maturity levels over time. Despite the relevance of the findings presented in this research, the cross-sectional approach of this study cannot capture the dynamics of cybersecurity implementation and adaptation. Future work should also explore how relevant organizational factors related to managers' leadership, organizational culture, or supply chain integration (Friday et al., 2024) influence firms' progression from low to high levels of cybersecurity implementation.

Second, specifically designed future research should evaluate the link between cybersecurity practices and performance metrics to establish whether and how certain cybersecurity practices have the potential to produce greater organizational resilience or improve operational or economic outcomes. Such studies can also explore potential moderating variables such as organizational culture, technological complexity, or supply chain integration (Lafuente et al., 2010; Friday et al., 2024). Third, further qualitative research is needed to increase our understanding of the barriers and enablers of cybersecurity adoption in small and large firms. The role of potential internal drivers (e.g., managerial knowledge, employee resistance) and external pressures (e.g., supply chain requirements, customer demands) can be included in such analysis.

Finally, this study focused on Costa Rican firms, and more studies across other developing and developed settings should be conducted to determine the generalizability of the findings and patterns observed in this study.

References

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, *4*(1), 65-88. https://doi.org/10.13052/jcsm2245-1439.414

Acs, Z. J., Lafuente, E., & Szerb, L. (2022). A note on the configuration of the digital ecosystem in Latin America. *TEC Empresarial*, *16*(1), 1-15. https://doi.org/10.18845/te.v16i1.5926

Anderberg, M.R. (1973). *Cluster Analysis for Applications*. Academic Press.

Bayon, M. C., Lafuente, E., & Vaillant, Y. (2016). Human capital and the decision to exploit innovative opportunity. *Management Decision*, *54*(7), 1615-1632. https://doi.org/10.1108/MD-04-2015-0130

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

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly*, *37*(2), 471-482. https://www.jstor.org/stable/43825919

Calinski, R.B., & Harabasz, J. (1974). A dendrite method for cluster analysis. *Communications in Statistics*, *3*(1), 1-27. https://doi.org/10.1080/03610927408827101

Chaudhary, V., Kaushik, A., Furukawa, H., & Khosla, A. (2022). Towards 5th generation AI and IoT driven sustainable intelligent sensors based on 2D MXenes and Borophene. *ECS Sensors Plus*, *1*, 013601. https://doi.org/10.1149/2754-2726/ac5ac6

Chaudhuri, A., Behera, R. K., & Bala, P. K. (2025). Factors impacting cybersecurity transformation: An Industry 5.0 perspective. *Computers & Security*, *150*, 104267. https://doi.org/10.1016/j.cose.2024.104267

Clemente-Almendros, J. A., Nicoara-Popescu, D., & Pastor-Sanz, I. (2024). Digital transformation in SMEs: Understanding its determinants and size heterogeneity. *Technology in Society*, *77*, 102483. https://doi.org/10.1016/j.techsoc.2024.102483

Dinkova, M., El-Dardiry, R., & Overvest, B. (2024). Should firms invest more in cybersecurity? *Small Business Economics*, *63*(1), 21-50. https://doi.org/10.1007/s11187-023-00803-0

Eller, R., Alford, P., Kallmünzer, A., & Peters, M. (2020). Antecedents, consequences, and challenges of small and medium-sized enterprise digitalization. *Journal of Business Research*, *112*, 119-127. https://doi.org/10.1016/j.jbusres.2020.03.004

Escribá-Carda, N., Redondo-Cano, A., & Escribá-Moreno, M. Ángeles. (2024). Firms' digital transformation and e-human resource management. A qualitative approach. *TEC Empresarial*, *18*(3), 103-128. https://doi.org/10.18845/te.v18i3.7289

Everitt, B.S. (1980). *Cluster Analysis*. Second edition. Heineman.

Friday, D., Melnyk, S. A., Altman, M., Harrison, N., & Ryan, S. (2024). An inductive analysis of collaborative cybersecurity management capabilities, relational antecedents and supply chain cybersecurity parameters. *International Journal of Physical Distribution & Logistics Management*, *54*(5), 476-500. https://doi.org/10.1108/IJPDLM-01-2023-0034

Greene, W. (2003). *Econometric Analysis*, 5th ed. Prentice Hall.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726. https://doi.org/10.1016/j.jisa.2020.102726

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics*, *3*(5), 97. https://doi.org/10.1007/s43546-023-00477-6

Heiding, F., Katsikeas, S., & Lagerström, R. (2023). Research communities in cyber security vulnerability assessments: A comprehensive literature review. *Computer Science Review*, *48*, 100551. https://doi.org/10.1016/j.cosrev.2023.100551

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165. https://doi.org/10.1016/j.dss.2009.02.005

Hoong, Y., & Rezania, D. (2024). Navigating cybersecurity governance: The influence of opportunity structures in socio-technical transitions for small and medium enterprises. *Computers & Security*, *142*, 103852. https://doi.org/10.1016/j.cose.2024.103852

James, T., Nottingham, Q., & Kim, B. C. (2013). Determining the antecedents of digital security practices in the general public dimension. *Information Technology and Management*, *14*, 69-89. https://doi.org/10.1007/s10799-012-0147-4

Lafuente, E., Acs, Z. J., & Szerb, L. (2024). Analysis of the digital platform economy around the world: A network DEA model for identifying policy priorities. *Journal of Small Business Management*, *62*(2), 847-891. https://doi.org/10.1080/00472778.2022.2100895

Lafuente, E., Alonso-Ubieta, S., Leiva, J. C., & Mora-Esquivel, R. (2021). Strategic priorities and competitiveness of businesses operating in different entrepreneurial ecosystems: a benefit of the doubt (BOD) analysis. *International Journal of Entrepreneurial Behavior & Research*, *27*(5), 1351-1377. https://doi.org/10.1108/IJEBR-06-2020-0425

Lafuente, E., Araya, M., & Leiva, J. C. (2022). Assessment of local competitiveness: A composite indicator analysis of Costa Rican counties using the 'Benefit of the Doubt' model. *Socio-Economic Planning Sciences*, *81*, 100864. https://doi.org/10.1016/j.seps.2020.100864

Lafuente, E., Bayo-Moriones, A., & García-Cestona, M. (2010). ISO-9000 certification and ownership structure: Effects upon firm performance. *British Journal of Management*, *21*(3), 649-665. https://doi.org/10.1111/j.1467-8551.2009.00660.x

Lafuente, E., & Sallan, J. M. (2024). Digitally powered solution delivery: The use of IoT and AI for transitioning towards a solution business model. *International Journal of Production Economics*, *277*, 109383. https://doi.org/10.1016/j.ijpe.2024.109383

Lafuente, E., Solano, A., Leiva, J. C., & Mora-Esquivel, R. (2019). Determinants of innovation performance: Exploring the role of organisational learning capability in knowledge-intensive business services (KIBS) firms. *ARLA-Academia Revista Latinoamericana de Administración*, *32*(1), 40-62. https://doi.org/10.1108/ARLA-10-2017-0309

Lafuente, E., Szerb, L., & Rideg, A. (2020). A system dynamics approach for assessing SMEs' competitiveness. *Journal of Small Business and Enterprise Development*, *27*(4), 555-578. https://doi.org/10.1108/JSBED-06-2019-0204

Lafuente, E., Vaillant, Y., & Leiva, J.C. (2018). Sustainable and traditional product innovation without scale and experience, but only for KIBS!. *Sustainability*, *10*(4), 1169. https://doi.org/10.3390/su10041169

Lafuente, E., Vaillant, Y., & Rabetino, R. (2023). Digital disruption of optimal co-innovation configurations. *Technovation*, *125*, 102772. https://doi.org/10.1016/j.technovation.2023.102772

Lederer, M., Schott, P., Huber, S., & Kurz, M. (2013). Strategic business process analysis: A procedure model to align business strategy with business process analysis methods. In: Fischer, H., Schneeberger, J. (eds) S-BPM ONE - Running Processes. S-BPM ONE 2013. *Communications in Computer and Information Science, vol 360*. Springer. https://doi.org/10.1007/978-3-642-36754-0_16

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports*, *5*, 100165. https://doi.org/10.1016/j.chbr.2021.100165

Long, J.S. (1997). *Regression Models for Categorical and Limited Dependent Variables*. Sage Publications.

Melville, N., Kraemer, K., & Gurbaxani, V. (2004). Information technology and organizational performance: An integrative model of IT business value. *MIS Quarterly*, *28*(2), 283-322. https://doi.org/10.2307/25148636

Mora-Esquivel, R., & Leiva, J.C. (2025). The role of digital service innovation strategy on SME performance: an international study. *Journal of Enterprise Information Management*. https://doi.org/10.1108/JEIM-02-2024-0099

Neri, M., Niccolini, F., & Martino, L. (2024). Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment. *Information & Computer Security*, *32*(1), 38-52. https://doi.org/10.1108/ICS-05-2023-0084

OECD (2017). Key issues for digital transformation in the G20. OECD Publishing. https://www.oecd.org/g20/key-issues-for-digital-transformation-in-the-g20.pdf

OECD (2024). New perspectives on measuring cybersecurity. OECD Digital Economy Papers, No. 366. https://www.oecd.org/en/publications/new-perspectives-on-measuring-cybersecurity_b1e31997-en.html

Porter, M. E., & Heppelmann, J. E. (2014). How smart, connected products are transforming competition. *Harvard Business Review*, *92*(11), 64-88. https://dialnet.unirioja.es/servlet/articulo?codigo=5544175

Rabetino, R., Kohtamäki, M., Foss, N. J., Rahman, N., & Huikkola, T. (2025). Microfoundations for business model innovation: Exploring the interplay between individuals, practices, and organizational design. *Journal of Product Innovation Management*, in press, https://doi.org/10.1111/jpim.12784

Rojas-Segura, J., Faith-Vargas, M., & Martínez-Villavicencio, J. (2023). Conceptualizing digital transformation using semantic decomposition. *TEC Empresarial*, *17*(3), 63-75. https://doi.org/10.18845/te.v17i3.6850

Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: A narrative review of cyber-security implications for Australian small businesses. *Computers & Security*, *109*, 102385. https://doi.org/10.1016/j.cose.2021.102385

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

Vaillant, Y., & Lafuente, E. (2024). Digital versus non-digital servitization for environmental and non-financial performance benefits. *Journal of Cleaner Production*, *450*, 142078. https://doi.org/10.1016/j.jclepro.2024.142078

Vaillant, Y., Lafuente, E., & Vendrell-Herrero, F. (2025). AI platforms as cooperation enablers favoring the development of strategic situating capabilities within solution delivery ecosystems. *Journal of Product Innovation Management* https://doi.org/10.1111/jpim.12807

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, *122*, 889-901. https://doi.org/10.1016/j.jbusres.2019.09.022

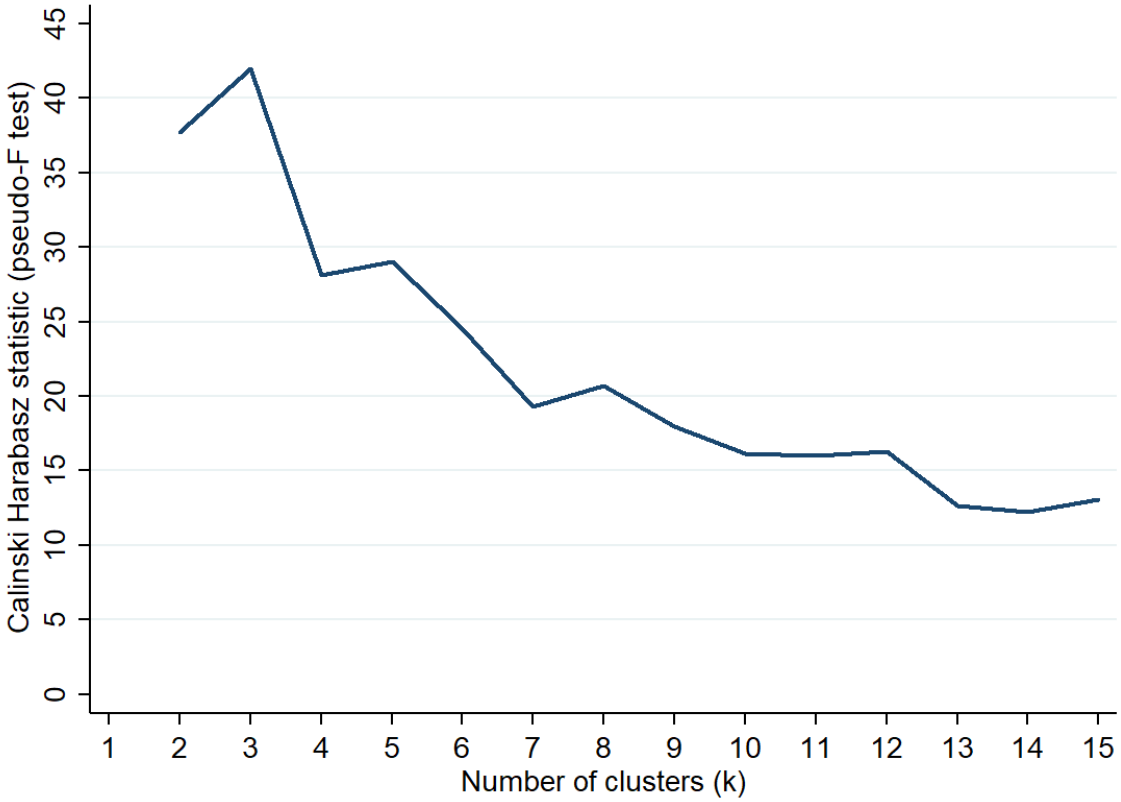
Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *23*(3), 191-198. https://doi.org/10.1016/j.cose.2004.01.012

Wilson, M., McDonald, S., Button, D., & McGarry, K. (2023). It won't happen to me: surveying SME attitudes to cyber-security. *Journal of Computer Information Systems*, *63*(2), 397-409. https://doi.org/10.1080/08874417.2022.2067791

Wong, L. W., Lee, V. H., Tan, G. W. H., Ooi, K. B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, *66*, 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520

Appendix

Appendix 1: Calinski and Harabasz statistic: Summary results



Source: Authors' elaboration based on the study data.