Technology in Society 78 (2024) 102670

Contents lists available at ScienceDirect

Technology in Society

journal homepage: www.elsevier.com/locate/techsoc

Exploring the economic role of cybersecurity in SMEs: A case study of the UK

Marta F. Arroyabe [a], Carlos F.A. Arranz [b], Ignacio Fernandez De Arroyabe [c,d], Juan Carlos Fernandez de Arroyabe [a,*]

[a] Essex Business School. University of Essex, UK
[b] Greenwich Business School, University of Greenwich, UK
[c] Computer Science Department, Loughborough University, UK
[d] Data Services, Commercial Banking, Lloyds Banking Group, London, UK

ARTICLE INFO

Keywords:
Cybersecurity
SME
Merit-good
Cybersecurity control
Cybersecurity management
Cybersecurity incidents

ABSTRACT

This study explores the economic role of cybersecurity in Small and Medium Enterprises (SMEs), situating cybersecurity within the framework of merit-goods within the economic theory of market failures and public goods. By examining 240 SMEs across the UK, the empirical findings of this investigation underscore its classification as a merit-good due to its extensive social benefits and the critical gap in its optimal provision. The results confirm the existence of market failure, such as the lack and asymmetry of information regarding cybersecurity, acknowledging the myopia and lack of information within SMEs, leading to suboptimal implementation of cybersecurity. Moreover, the lack of optimal implementation is evidenced by the findings indicating that neither cybersecurity incidents nor cybersecurity impacts in SMEs drive the implementation of cybersecurity. Additionally, we observe that implementation is more focused on control systems than on management systems, which is a significant differentiating factor from large enterprises. The study contributes theoretically by framing cybersecurity as a merit-good, provides managerial insights into SME cybersecurity practices, and emphasizes the importance of nuanced policies to bridge the implementation gap.

1. Introduction

In the contemporary business landscape, cybersecurity is of vital importance for businesses, encompassing a set of practices, technologies, and measures designed to safeguard systems, networks, data, and software programs from attacks, damages, unauthorised access, information robbery, and other digital threats [1,2]. As businesses increasingly rely on technology for critical operations, cybersecurity has become a fundamental aspect of their continuous functioning [3]. This is because cybersecurity is essential for protecting a company's digital assets, ensuring business continuity, and maintaining customer trust in an increasingly digitized and interconnected business environment [4].

Small and Medium-sized Enterprises (SMEs) are trailing behind larger businesses in the adoption of digital technologies and cybersecurity [5]. The digital gap has been further widened by the COVID-19 crisis, with SMEs expected to decrease their IT expenditures, while large firms are anticipated to increase theirs [6]. This discrepancy negatively impacts cybersecurity in SMEs compared to their larger counterparts. In this context, a crucial question arises regarding the relationship between cybersecurity and SMEs, considering the economic and social significance of SMEs [7].[1] This is particularly remarkable in the European context, especially in the UK, where their substantial contributions to GDP, employment, and consumption stand out [8]. In this regard, academia has not been indifferent to addressing this relationship, finding that this connection poses challenges and contradictions, which do not shed light on the economic and managerial role that cybersecurity represents in the SME.

Firstly, as SMEs undergo digitalization, their exposure to cybersecurity incidents significantly increases [9]. The adoption of digital technologies and internet connectivity expands the attack surface, making cybersecurity crucial for protecting digital assets and ensuring business continuity. Despite this reinforced exposure to potential

* Corresponding author.
E-mail addresses: mf17255@essex.ac.uk (M.F. Arroyabe), c.fernandezdearroyabearranz@greenwich.ac.uk (C.F.A. Arranz), I.Fernandez@lboro.ac.uk, ignacio.fernandez-de-arroyabe@lloydsbanking.com (I. Fernandez De Arroyabe), jcfern@essex.ac.uk (J.C. Fernandez de Arroyabe).

[1] SMEs represent about 90 % of businesses and more than 50 % of employment worldwide [51].

https://doi.org/10.1016/j.techsoc.2024.102670
Received 12 December 2023; Received in revised form 9 July 2024; Accepted 26 July 2024
Available online 26 July 2024

cybersecurity incidents, some senior managers of SMEs may hold a mistaken perception that their businesses are not susceptible to cybersecurity incidents [10]. This misconception can lead to insufficient attention and underinvestment in cybersecurity.

Secondly, in contrast to this misconception, the reality unveils that SMEs are susceptible to cybersecurity incidents [11,12]. Statistics indicate that 81 % of cybersecurity incidents affect SMEs, with 60 % of them experiencing a cybersecurity breach in the past year [13]. Common incidents include indiscriminate attacks, phishing, and the misuse of IT infrastructure. Additionally, given their integral role in supply chains, SMEs can become attractive targets for cybercriminals aiming to gain access to larger enterprises [14].

Lastly, the literature has been characterised by its scarcity, especially if we compare it with large companies, by a diversity of approaches, most of which have a marked technical nature of cybersecurity in SMEs [12,15,16], leaving away the economic and management perception of cybersecurity. While the cybersecurity literature for large companies has considered cybersecurity as a crucial asset [16,17], emphasizing the importance of investment from both operational and reputational perspectives, the role of cybersecurity in SMEs has not been clarified. This lack of clarity hinders the understanding of what drives implementation or how it is managed [1]. Thus, investment in cybersecurity and effective management can be viewed as preventive and proactive measures to protect reputation, ensure business continuity, and facilitate participation in business networks [18,19].

Our paper aims to explore the economic and management role of cybersecurity in SMEs. In this context, we focus on SMEs in the United Kingdom, using a database of 240 SMEs distributed throughout the country. As a theoretical framework, we employ the economic theory of market failures and public goods [20,21], with cybersecurity assumed as a merit-good. Traditionally, cybersecurity has been treated as a public good [22–24], because cyber threats do not only affect the target company of the attack but can also spread through networks and affect multiple users simultaneously, turning the cyber incident into damage not only for the company but for society in general. However, considering cybersecurity as a merit-good not only allows us to view it as a public good but also enables us to investigate the characteristics of how cybersecurity is being managed in companies. Firstly, the conceptualization of merit-goods indicates that they may not be consumed optimally if left solely in the hands of the market [25,26]. This is due to a lack of complete recognition of their benefits by organizations and individuals. Therefore, our research will empirically address how cybersecurity in SMEs is managed and implemented and what factors affect this suboptimal implementation. Thus, the cybersecurity literature in SMEs suggests that these organizations, often due to a myopia in the perception of cybersecurity risk, do not consider implementing cybersecurity crucial [7]. Last, this theoretical framework supports the notion that government intervention may be necessary to ensure the adequate provision and consumption of merit-goods [26]. In this context, our research addresses how government intervention affects the management of cybersecurity in SMEs.

For this study, we will merge descriptive analysis with regression and cluster analysis in a exploratory analysis. This strategic combination of statistical methods offers several substantial advantages. On one hand, it enables us to explore causal relationships between variables. On the other hand, cluster analysis empowers us to uncover patterns and segment data into homogeneous sets, thereby enriching our understanding of the studied population and facilitating the identification of relevant subgroups.

2. Conceptualization and research model

2.1. Digitalization and cybersecurity

The relationship between cybersecurity and digitalization is intrinsically connected, evolving in tandem with the increasing reliance on digital technologies across various sectors [18,27–31]. As organizations embark on digital transformation journeys, incorporating technologies such as cloud computing, the Internet of Things (IoT), and artificial intelligence, the attack surface for potential cybersecurity incidents expands significantly. Digitalization brings forth unprecedented efficiency and connectivity, but it also exposes systems, networks, and sensitive data to new and sophisticated cybersecurity risks [32–34]. Cybersecurity plays a pivotal role in this landscape, serving as the safeguard against unauthorised access, data breaches, and other malicious activities that could compromise the integrity, confidentiality, and availability of digital assets [19].

Organizations face an escalating and diversifying landscape of cybersecurity threats, continually growing in sophistication [7,9,19,35]. Various types of cybersecurity attacks, employing techniques such as phishing, malware, web attacks, and the exploitation of IT system vulnerabilities, are identified in the literature. ENISA [36] classifies cyberattacks, highlighting malware as constituting 30 % of all incidents. Additional threats encompass website and domain attacks targeting personal information and banking details, alongside phishing endeavors aiming to impersonate identities and deploy malware. Beyond external threats, internal staff can inadvertently or deliberately cause security breaches, a concern emphasized by ENISA [36], indicating that 77 % of data leaks in firms originate from internal sources. Also, these cybersecurity incidents impact SMEs, causing disruptions that hinder daily operations and impede staff responsibilities [7]. The consequences extend beyond economic losses, encompassing potential harm to the reputation and legal liabilities of SMEs. Instances such as data breaches and non-compliance with the General Data Protection Regulation (GDPR) can result in legal repercussions and financial penalties for these enterprises.

In the organizational context, the implementation of cybersecurity measures is initiated to safeguard IT systems. This involves a comprehensive set of measures, strategies, and procedures designed to mitigate the risks and vulnerabilities associated with information systems [4]. The literature emphasizes a spectrum of operational, strategic, and organizational actions in this realm (ISO, 2016; [17]). Operational cybersecurity control mechanisms involve the establishment of routines and procedures, encompassing activities like software updates, the utilization of firewalls, identification routines, and network security measures. Additionally, secure communication methods such as VPNs and data encryption may be integrated [7]. On a strategic and organizational level, companies implement cybersecurity management measures, assigning dedicated teams for information security management, formulating policies, and developing systems for assessing cybersecurity risks (e.g., ISO 27000s, Cyber Essentials). Cybersecurity concerns are also incorporated into senior management meetings within companies (ISO, 2016; [17]). In this landscape, cybersecurity standards, such as ISO 27000 [4] and UK Cyber Essentials [37], emerge as facilitative mechanisms. These standards provide guidelines and best practices to enhance cybersecurity measures, ensuring the security of systems, data, and networks. The implementation of such standards proves instrumental for SMEs in establishing a robust cybersecurity framework, underscoring their commitment to protecting sensitive information and mitigating cyber risks.

2.2. The economic role of cybersecurity in SMEs

In this paper, we posit that cybersecurity in SMEs can be regarded as a merit good. The conceptualization of this investigation is rooted in the economic theory of market failures and public goods, particularly in the definition of merit goods [20,21]. In this context, merit-goods stand out as commodities that generate positive external benefits for society, and their consumption or provision is associated with the enhancement of overall well-being [25,26]. Following these authors, a merit-good is defined as a good that contributes positive benefits to society and may not be consumed optimally if left entirely to the market due to

individuals' lack of complete recognition of its broader benefits. The theory suggests that in the absence of intervention, markets may not efficiently allocate these goods because individuals may not fully internalize the social benefits they generate [20]. This theoretical framework supports the notion that government intervention may be necessary to ensure the proper provision and consumption of merit-goods, thereby contributing to a more equitable distribution of social benefits [26].

In this context, assuming the conceptualization of cybersecurity as a merit-good implies that it may not be consumed optimally if left entirely to the market due to the lack of complete recognition of its benefits [25,26]. Regarding cybersecurity in SMEs, the literature suggests that organizations often invest less than necessary in cybersecurity compared to the socially optimal level [7]. Various market failures can contribute to this underinvestment, such as information asymmetries. The cybersecurity literature has highlighted how SMEs may not fully comprehend their cybersecurity risks or the benefits of cybersecurity investments [1,12].

Moreover, merit-goods are considered public goods and require intervention by administrations to achieve optimal consumption [26]. Firstly, cybersecurity exhibits characteristics of a public good as it is non-rivalrous (one person benefiting from cybersecurity does not reduce its availability for others) and non-excludable (it is difficult to prevent non-paying individuals from benefiting) [14,18]. Secondly, cybersecurity provides significant positive externalities by safeguarding critical infrastructure, reducing cybercrime, and minimizing disruptions caused by cybersecurity incidents; however, various market failures suggest that organizations are likely to invest little in its absence of public policies. In this regard, administrations intervene by developing standards, such as the ISO 27.000 family or Cyber Essentials, to address the lack of investment in cybersecurity within organizations [4,37].

2.3. Research questions: cybersecurity management in SMEs

Therefore, assuming that cybersecurity in SMEs could be considered a merit-good, we will pose research questions to explain how it is being implemented and managed. Building on the literature and previous definitions from the earlier section, we will present our research model, which includes four research questions. These questions will allow us to explore how cybersecurity is managed in SMEs and conceptualize it as a merit good. From the previous section, we have identified that a merit good is characterized by users' lack of information about the benefits of cybersecurity. Additionally, we will examine the drivers that motivate SMEs to implement cybersecurity, how this implementation is managed, and, finally, analyse the role of administration.

The first characteristic of merit-goods is the lack of information and asymmetry regarding this commodity, leading to suboptimal consumption. This is because the literature has noted that SMEs suffer from myopia concerning cybersecurity, stemming from the lack of information about cybersecurity incidents [7,12]. Moreover, Fernandez de Arroyabe and Fernandez de Arroyabe [7] have highlighted the limited knowledge and involvement of senior managers in SMEs in cybersecurity, noting the low level of cybersecurity updates provided to senior managers of SMEs [13]. Additionally, senior managers in SMEs do not consider themselves targets of cybersecurity attacks, leading to a lack of concern about cybersecurity information. However, the literature has emphasized that cybersecurity attacks are becoming increasingly sophisticated and covert, which can impede detection by SMEs, and that SMEs are targets of cybersecurity attacks [11,36]. Therefore, we propose a first research question.

Research Question (RQ1). Do SMEs experience a lack of information and asymmetry regarding cybersecurity?

In response to the previous research question concerning the lack of cybersecurity information in SMEs, it is essential to formulate a question that addresses the drivers for the implementation of cybersecurity measures.

First, it is important to note that the literature on cybersecurity drivers is diverse, encompassing a wide range of perspectives. Thus, the literature identifies several key drivers for cybersecurity in companies: organizational awareness and commitment (for example, [38]), regulatory requirements [39], the increasing sophistication of cyber threats [40], technological advancements [41], and industry best practices [42]. Additionally, organizational culture and employee training are crucial for effective cybersecurity [43]. A comprehensive approach, influenced by both internal and external factors, is necessary for robust cybersecurity management.

Second, in this paper, we can consider three potential drivers. The first driver can be the digital transformation of SMEs. Digitalization involves the interconnection of SMEs' devices, increasing exposure to cybersecurity incidents [2,31]. Therefore, it is expected that certain SMEs may consider implementing cybersecurity to protect themselves during digital transformation. The second driver can be the occurrence of cybersecurity incidents. SMEs are targets of both automated and targeted attacks, which can impact their operations [1]. Additionally, the inappropriate use of IT devices in the organization can result in cyber incidents. Hence, cyber incidents can act as a catalyst for the implementation of cybersecurity. Lastly, SMEs may have suffered economic damages due to cyber incidents [1]. Issues such as business disruptions, data theft, and reputation problems, among others, can be the main challenges posed by cybersecurity incidents. Therefore, we propose the following question.

Research Question (RQ2). What drives the implementation of cybersecurity in SMEs?

As we have seen earlier, a merit-good is characterized by suboptimal consumption [25,26]. In this context, cybersecurity in SMEs, as a merit commodity, can be characterized as a suboptimal level of implementation. Thus, as previously discussed, the implementation of cybersecurity measures involves a comprehensive set of measures, strategies, and procedures designed to mitigate the risks and vulnerabilities associated with information systems. The literature emphasizes a spectrum of operational, strategic, and organizational actions in this domain [7]. Therefore, SMEs can implement operational cybersecurity control mechanisms by establishing routines and procedures, covering activities such as software updates, the use of firewalls, identification routines, and network security measures, for example. Additionally, SMEs can strategically and organizationally develop a series of cybersecurity management measures by assigning dedicated teams to information security management, formulating policies, and developing systems to assess cybersecurity risks. Therefore, we pose the following question.

Research Question (RQ3). How is cybersecurity implemented in SMEs?

Finally, merit-goods can be considered public goods due to the social benefits they generate [25,26]. In this context, the intervention of administrations is expected to address their deficiency. In the case of cybersecurity in SMEs, we can highlight the benefits it brings to businesses by mitigating cybersecurity incidents and avoiding operational and reputational problems, for example. Moreover, the implementation of cybersecurity has significant social benefits, enabling the proper functioning of business networks [32]; therefore, we can consider cybersecurity as a public good, susceptible to being promoted by institutions.

In this regard, the literature has emphasized that institutions intervene both to address negative externalities and to guide organizational behaviours [4,17]. In the case of cybersecurity, the predominant use of standards emerges, determining the cybersecurity management systems in companies, as seen in ISO 27,000 or Cyber Essentials. Therefore, we pose the following question.

Research Question (RQ4). How do standards affect the

implementation of cybersecurity in SMEs?

3. Methodology and data

3.1. Data

For this study, we conducted a survey targeting UK SMEs. The unit of analysis is the organization, and for this research, we define SMEs based on size, typically ranging from 1 to 250 employees. The sample was obtained using the Government's Inter-Departmental Business Register (IDBR), which encompasses UK organizations across all sectors. To select the population, we employed random-probability sampling to mitigate selection bias, consistent with prior studies, aiming for a population of 1000 SMEs.

Fieldwork was piloted between February and May 2022, with the analysis period spanning from 2019 to 2022. The survey was conducted online, comprising two waves. Following clarification of received questionnaires and the removal of non-answer and incomplete responses, the final sample dataset for the study comprises 239 SMEs. The survey is statistically representative of UK SMEs across various sizes and sectors. To confirm this, we conducted T-tests to ascertain if there were significant differences between the population and the final sample concerning size and sectors, resulting in no significant bias.

The distribution of the sample is made up of a high percentage (77.8 %) of micro-enterprises (1–9 employees); with less representation (16.4 %) of small companies (10–49 employees), and lastly, medium-sized companies (50–249 employees), with 5.8 %. Regarding the sectoral distribution, following SIC classification, we find 19 sectors represented, finding a very balanced sample. Thus, the most represented sectors are *professional, scientific and technical activities* (SIC: 74909), *agents involved in the sale of a variety of goods* (SIC: 46190), *manufacture of loaded electronic boards activities* (SIC: 26120), *business* support *service activities* (SIC: 82990), *human health activities* (SIC: 86900), *amusement and recreation activities* (SIC: 93290), and *repair of computers and peripheral equipment* (95110). Finally, we have found a homogeneous geographical distribution of the sample in the UK.

Also, we checked the robustness of the survey and the results. Firstly, we analysed the responses obtained in the two waves, and we did not find significant discrepancies between the two waves. Second, we performed checks of the survey to verify the robustness of the questionnaires and answers, testing the common method variance and common method bias, following the method of Podsakoff et al. [44]. The analysis has identified nine distinct constructs that collectively account for 64.089 % of the variance. The first factor accounts for 17.420 % of the variance, which is in line with the recommended threshold of 50 %. Consequently, we can infer that common method variance and common method bias are not significant concerns in our findings.

3.2. Measures

The first variable of our research captures digital technologies. To do this and in line with the literature, we pose a multi-item question, using a relation of emerging technologies such as big data, cloud technology, artificial intelligence and machine learning (AI/ML), robotics, data analytics and blockchain [45,46]. The question posed is: which of the following *digital technologies* has your enterprise adopted?, containing multi-item options: i) Artificial intelligence; ii) Cloud computing; iii) Robotics; iv) Smart devices; v) Big data analytics; vi) High-speed infrastructure; and vii) Blockchain. To assess the degree of *digital technologies* in SMEs, we constructed a new variable, formulated as a cumulative index of the six types of digital technologies.

The second group of variables refers to the management of cybersecurity in SMEs. Previous works [7] classify cybersecurity actions into two variables. The first variable refers to the cybersecurity processes and routines used in the period 2019 to 2022 (*cybercontrols*), using a multi-item question. The items chosen in this question are: i) Regular software updates (including patching); ii) Encrypting or securing data; iii) Malware protection; iv) Use of VPN; v) Firewalls and network security; vi) Identity and Access Management; vii) Physical security controls on firm -owned devices; viii) Only allowing access via firm-owned devices; ix) A segregated guest wireless network; and x) Regular backing up data securely. The second variable refers to the strategic and organizational measures in the implementation of cybersecurity in SMEs (*cybermanagement*), during the period 2019 to 2022. The question is multi-item: i) An outsourced provider that manages your cybersecurity; ii) Staff members with information security or governance responsibilities; iii) A formal policy or policies in place covering cybersecurity risks; iv) Invested in threat intelligence; v) An independent cybersecurity assessment; vi) Any business-as-usual health checks that are undertaken regularly; and vii) Formal cybersecurity discussions with the CEO, board or equivalent. In line with previous variables, tanto *cybercontrols* como *cybermanagement* are created as a cumulative index.

The next variable refers to the level of cybersecurity impacts of an economic and management nature produced in SMEs (*cyberimpacts*). In line with the literature by Fernandez de Arroyabe and Fernandez de Arroyabe [7], we consider the following impacts generated: i) Stopped the business-as-usual activities; ii) Negative impact on the revenue or share value; iii) Repair or recovery costs; iv) Fines from regulators or authorities or associated legal costs; and v) Reputational damage and loss of customer trust. In alignment with the preceding variables, *cyberimpacts* is constructed as a cumulative index.

The next variable shows the main cybersecurity incidents (*cyberincidents*). The question included in the questionnaire is; has any of the following cybersecurity incidents (successful or unsuccessful) happened to your organisation in the last 12 months? The answer is multi-item: i) Phishing or spear phishing; ii) ransomware; iii) viruses, spyware or malware; iv) attacks that try to take down your website or online services; v) unauthorised use of computers, networks or servers by staff, even if accidental (insider incident); vi) unauthorised use or hacking of computers, networks or servers by people outside your organisation; vii) hacking or attempted hacking of online bank accounts; and viii) denial of service (DoS or DDoS). En linea con previas variables, la variable cyberincidents es construidad com un cumulative index.

The last variable is the possession of the cybersecurity standards (*cyberstandards*). The question posed was: Has your organisation adopted the International Standard for Information Security Management (ISO 27001) or Cyber Essential? The variable is measured by a Likert scale from 1 to 4, being 1 (No, I am not aware of these certifications); 2 (No, and do not intend to do so); 3 (No, but is intending to do so); and 4 (Yes).

3.2.1. Control variables

We use three control variables in our investigation, which are: the size of the company, growth, and the degree of cybersecurity competencies.

The first control variable is the size of the SMEs. We use a multi-item scale to classify the companies as follows: i) 1 to 9 employees; ii) 10 to 49 employees; and iii) 50 to 250 employees.

The second control variable is the growth of SMEs. The question is: "Since 2017, how much has your organization grown, if at all, in terms of turnover?" The question has multiple options: i) It has not grown; ii) Grown by less than 10 % per year; iii) Grown by between 10 and 20 % per year; and iv) Grown by more than 20 % per year.

The last control variable is the degree of digital competencies. The question is to what extent do the following digital skills and competencies are missing in your organisation? The answer is multi-item con diverse digital competencies: i) Cybersecurity; ii) Data analysis; iii) Database management; iv) Digital leadership; v) Digital project management and strategy; vi) Software development; and vii) Website development. The answer is a Likert scale from; Extremely unlikely; Somewhat unlikely; Somewhat likely; Extremely likely.

4. Analysis and results

Previously to the analysis, we checked the robustness of the survey and the results. Firstly, we analysed the responses obtained in the two waves, and we did not find significant discrepancies between the two waves. Second, we performed checks of the survey to verify the robustness of the questionnaires and answers, testing the common method variance and common method bias, following the method of Podsakoff et al. [44]. The analysis has identified nine distinct constructs that collectively account for 64.089 % of the variance. The first factor accounts for 17.420 % of the variance, which is in line with the recommended threshold of 50 %. Consequently, we can infer that common method variance and common method bias are not significant concerns in our findings.

Before the analysis of the research questions, we obtained some descriptive data on the analysis variables, to contextualize cybersecurity and the digitalization of SMEs (Table 1). Firstly, regarding cybersecurity control systems, we observe that 40 % of the SMEs adopted software updates, firewalls, and banking up, as cybersecurity control systems; however, the least incorporated are VPN, access management, and network segregation, which are adopted in less than 20 % of companies. In line with the previous variable, we have analysed the degree of penetration of control systems (*cybercontrol*), measured as a cumulative index of the cybersecurity control systems. The results show that SMEs combine various cybersecurity control mechanisms, in a minimum number of 4–7, most frequently used, such as software updates, firewall and malware protection, combined with access management measures, physical controls or VPN. Regarding cybersecurity management systems, in general, only 10 % of companies use some *cybersecurity management*, such as outsourcing management, the assignment of personnel to assume these responsibilities or the setting of policies for cybersecurity. Additionally, from our results, we observe that there is very little use of several systems simultaneously (*cybermanagement*), such as the existence of personnel and discussions on the board of companies, or the establishment of cybersecurity policies. Secondly, regarding the level of adoption of digital technologies by SMEs, our results show that the most frequently adopted digital technology is cloud computing, accounting for 49.8 % of cases. AI, big data, smart devices, and high-speed infrastructure are adopted to a lesser degree, with a prevalence of 10 % among SMEs. The adoption of robotics and blockchain is relatively infrequent. Moreover, we have analysed the level of digitalization, which is considered the degree of penetration of digital technologies. The variable *digitalization* was constructed as a cumulative index of seven types of digital technologies (AI, cloud computing, robotics, smart devices, big data analytics, high-speed infrastructure, and blockchain). The results indicate that the degree of penetration of digital technologies adopted by SMEs is low. Only 13.8 % of companies adopt two or more digital technologies, while 7.9 % adopt three or more technologies.

Regarding the first research question (RQ1), which explores the availability and asymmetry of information within SMEs concerning cybersecurity, we have examined information related to cyber incidents that SMEs may experience (Table 2). We have assessed the level of knowledge regarding the impact of these cybersecurity incidents and their impacts on SMEs. When it comes to cybersecurity incidents (*cyberincidents*), we observe a low response rate. Except for 20.5 % of SMEs that have encountered issues with phishing and 14.2 % with viruses, the responses for all other incidents are below 10 %. Along the same lines, we note a limited response regarding cybersecurity impact (*cyberimpact*). Specifically, the most common impact reported is the interruption of activities and associated costs resulting from incident damages. Less frequently mentioned are impacts on the firm's reputation or issues with regulatory authorities (see Table 3).

Regarding RQ2, which investigates the factors driving the implementation of cybersecurity in SMEs, we have analysed three potential drivers: digitalization, cybersecurity incidents, and cybersecurity impact. Before conducting the regression analysis, we explored the behaviour of the sample concerning these three drivers. We conducted an exploratory representation of the variables based on the level of digitalization (Fig. 1). Fig. 1 represents the level of digitalization on the horizontal axis (digitalization range: 0 to 6) and the mean values of the cybersecurity control, cybersecurity management, cybersecurity impact, and cybersecurity incidents variables on the vertical axis for each level of digitalization. The graph indicates that both cybersecurity control and management systems exhibit an increasing trend with digitalization. However, there is no significant variability in cybersecurity impact and cybersecurity incidents concerning digitalization. Moreover, in Fig. 1, we observe a drastic drop when the level of digitalization is 5, corresponding to companies with five digital technologies implemented. As seen earlier, the average number of technologies incorporated by companies is one or two, making the number of companies incorporating 5 or more statistically insignificant.

Next, we conducted an exploratory analysis to classify the SMEs into different groups based on their degree of cybersecurity. Then, we analysed if there are significant differences in the relationship between

Table 2
Cybersecurity incidents and cybersecurity impact variables.

CYBER INCIDENTS			CYBERIMPACT		
Variables	*Frequency*	*Per cent*	*Variables*	*Frequency*	*Per cent*
PHISHING	49	20.5	STOPPED BUSINESS	12	5.0
RANSOMWARE	10	4.2	NEGATIVE REVENUE	4	1.7
VIRUSES	34	14.2	REPAIR COSTS	10	4.2
ATTACKS WEBSITE	20	8.4	AUTHORITIES	2	.8
UNAUTHORISED USED	4	1.7	REPUTATIONAL	5	2.1
HACKING	11	4.6			
HACKING BANK	10	4.2			
DoS	7	2.9			

Table 1
The descriptive results of cybersecurity management in SMEs.

CYBERCONTROL			CYBERMANAGEMENT			DIGITAL TECHNOLOGIES		
Variables	Frequency	Per cent	Variables	Frequency	Per cent	Variables	Frequency	Per cent
SOFTWARE UPDATE	116	48.5	OUTSOURCING	25	10.5	CLOUD	119	49.8
ENCRYPTING	74	31.0	STAFF	36	15.1	AI	25	10.5
MALWARE PROTECTION	94	39.3	POLICY	34	14.2	SMART DEVICES	23	9.6
VPN	61	25.5	THREAT INTELLIGENCE	16	6.7	ROBOTICS	12	5.0
FIREWALLS	103	43.1	ASSESSMENT	16	6.7	BIG DATA	26	10.9
ACCESS MANAGEMENT	62	25.9	CHECKS	32	13.4	BLOCKCHAIN	11	4.6
PHYSICAL CONTROLS	48	20.1	BOARD DISCUSSION	25	10.5	HIGH-SPEED	22	9.2
OWNED DEVICES	45	18.8						
SEGREGATED NETWORK	42	17.6						
BACKING UP	97	40.6						

Table 3
Mean values of variables for Clusters.

VARIABLES	RANGE		CLUSTER 1		CLUSTER 2	
	Minimum	Maximum	Mean	Std. D.	Mean	Std. D.
DIGITALIZATION	0.00	6.00	1.31	1.13	0.57	1.08
CYBERCONTROLS	0.00	10.00	6.57	1.85	0.29	0.77
CYBERMANAGEMENT	0.00	7.00	1.49	2.08	0.18	0.84
CYBERIMPACT	0.00	5.00	0.21	0.63	0.07	0.48
CYBERINCIDENTS	0.00	8.00	1.18	1.49	0.13	0.76
RESTORE TIME	1.00	6.00	1.52	0.93	3.00	2.00
TOTAL SMES			**107**		**132**	

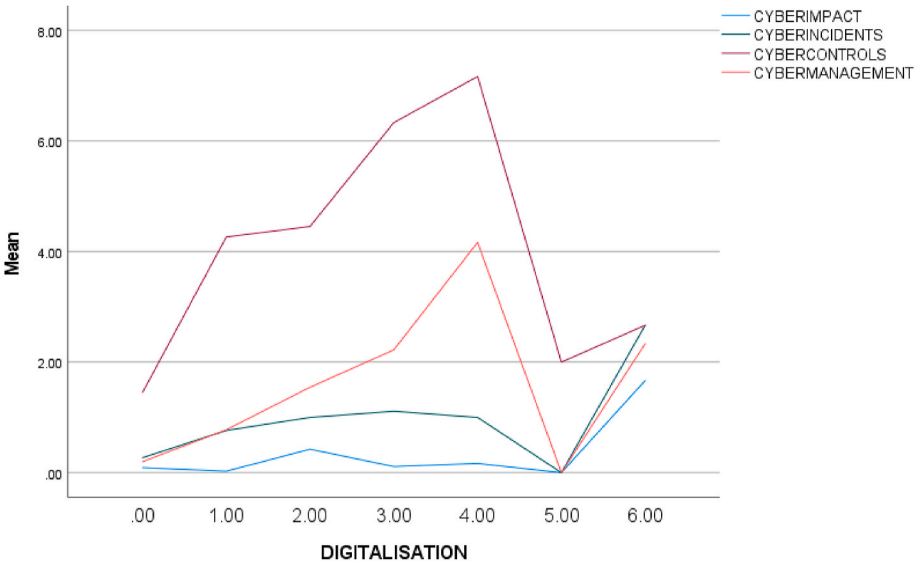

Fig. 1. Representation of the variables based on the level of digitalization.

cybersecurity based on the group to which the SME belongs. Using the K-mean Cluster as a statistical model [47,48], we have proceeded in two stages. First, the K-means algorithm considers input variables that are significant in the behaviour of cybersecurity and digitalization (*cybersecurity control, cybersecurity management, digitalization*). Second, we proceed to the choice of the most robust solution, using Silhouette analysis [47,48]. This analysis allows us to determine the robustness of the cluster solution, the cohesion of each cluster and the separation of the groups. Silhouette index takes values in the interval [−1, 1], with values closer to 1 being the most robust solution. After proceeding to obtain the Silhouette index, the two clusters solution has a higher value of Silhouette (0.63). Furthermore, we performed a complementary analysis, using the Schwarz' Bayesian Criterion [49,50], and the results confirm that the solution two clusters are the most robust in terms of cohesion and separation. The results of the K-mean cluster analysis show that SMEs are grouped into two clusters. Additionally, we have performed a robustness check of the analysis, using ANOVA analysis, and the results show a significant difference in the degree of cybersecurity and digitalization as a function of the cluster variable. In Table 2, we present the mean values of each variable used in the analysis for each cluster. Overall, we observe that Cluster 1 has a higher level of cybersecurity and digitalization compared to Cluster 2.

Having identified heterogeneous groups, we proceeded to analyse the impact of the three drivers on the implementation of cybersecurity.

Table 4
Regression Analysis Cybersecurity control (CLUSTER 1).

Variables	Model 1	Model 2	Model 3	Model 4	Model 5	VIF
Size	1.000[c] (.317)	1.003[c] (.325)	1.005[c] (.315)	.930[c] (.326)	.957[c] (.336)	1.140
Growth	.277[b] (.074)	.178[b] (.076)	.248[b] (.074)	.266[b] (.074)	.163[b] (.077)	1.115
Competencies	−0.071[b] (.036)	−0.097[b] (.037)	−0.089[b] (.039)	−0.072[a] (.037)	−0.098[b] (.039)	1.272
DIGITALIZATION		.398[b] (.165)			.390[b] (.167)	1.127
CYBERIMPACT			.531 (.292)		.195 (.341)	1.537
CYBERINCIDENTS				.208 (.121)	.182 (.142)	1.430
−2 Log Likelihood	326.248	348.956	340.359	358.997	360.051	
Chi-Square	16.220	22.521	18.405	18.836	25.524	
Sig.	.001	<.001	.001	<.001	<.001	
Cox and Snell	.144	.195	.162	.166	.218	
Nagelkerke	.148	.199	.166	.170	.223	
McFadden	.041	.057	.047	.048	.065	

[a] $p < 0.05$.
[b] $p < 0.01$.
[c] $p < 0.001$.

Firstly, concerning Cluster 1, which comprises 107 SMEs characterized by a higher level of digitization and cybersecurity implementation, Tables 4 and 5 present the analysis of regression. In this case, we use Ordinal Logistics Model as econometric model. In Table 4, we used *cybersecurity control* as the dependent variable, and in Table 5, *cybersecurity management*, with *digitalization, cyber impact, cyber incidents*, and three control variables as independent variables. Thus, it is confirmed that digitization has a positive impact on both the probability of implementing cybersecurity controls (Model 5: $\beta = -0.390$; $p < 00.001$) and cybersecurity management systems (Model 5: $\beta = -0.661$; $p < 00.001$). However, our results are not statistically significant for the case of cybersecurity incidents and cybersecurity impact in both variables.

In Tables 6 and 7, we present the results of the regression analysis for Cluster 2, which exhibits a low level of cybersecurity and digitization, comprising 132 SMEs. Consistent with previous analysis, we proceed to analyse using the Ordinal Logistic Regression Model. In Table 6, we used *cybersecurity control* as the dependent variable, and in Table 7, *cybersecurity management*, with *digitalization, cyber impact, cyber incidents*, and three control variables as independent variables. Thus, we observe that none of the three drivers have an impact on the implementation of cybersecurity control and cybersecurity management.

Regarding RQ3, which analyses how cybersecurity is implemented in SMEs, we observe significant differences between Cluster 1 and Cluster 2 (Table 7). Firstly, Cluster 1, composed of 107 SMEs, has an average level of digitalization of 1.31, indicating that each SME, on average, adopts between 1 and 2 digital technologies within a maximum range of six. Thus, in this cluster, 72.0 % of them adopt cloud computing, to a lesser extent big data (17.2 %), and high-speed infrastructure (16.8 %). The adoption of smart devices, robotics, AI, or blockchain is less frequent. As for protection methods, we observe that *cybercontrols* have an average score of 6.57, while *cybermanagement* has a score of 1.49. This is, in 95.3 % of the cases, SMEs in this cluster maintain software updates and use encryption software (68.2 %), firewalls (88.8 %), malware protection (84.1 %), or backup solutions (86.9 %). To a lesser extent, they employ network segregation and access control, for example. Regarding cybersecurity management in terms of procedures and routines, it decreases in comparison to control systems (average: 1.49). The most frequently used practices include staff allocation (29.9 %), periodic checks (26.2 %), board discussions (20.6 %), and the use of cybersecurity policies (27.1 %). Finally, the restoring time is 1.52, indicating that, on average, cybersecurity incidents are repaired in less than one working day. Second, Cluster 2, contains 132 SMEs, we see that the level of digitalization is almost non-existent, with an average score of 0.57 on a scale of 0–6. Thus, when SMEs have adopted any digital technology, it is cloud computing (31.7 %). In terms of the implementation of cybersecurity mechanisms, it is very limited, primarily based on software updates (10.6 %), and firewalls (8 %). Regarding organizational procedures and routines, the allocation of specific personnel (3.0 %) and outsourcing (3.8 %) are the most common practices. As for the restoration time of SME activity, the average corresponds to a period between 1 day and one week. It should be noted that the response obtained is from less than 9 SMEs (6.8 %).

Finally, RQ4 aimed to explore the effect of institutional impulse on the implementation of cybersecurity in SMEs (Tables 8 and 9). We can observe that, in the case of Cluster 1, with a higher level of implementation, approximately 18.7 % have implemented Cyber Essentials standards, and to a lesser extent, the implementation of ISO 27000 is at 15.1 %. Regarding the intention to implement, we observe that the obtained response is 11.2 % for ISO and 13.1 % for Cyber Essentials. In the case of Cluster 2, characterized by a low level of cybersecurity and digitalization, the level of implementation is very scarce. As for the implementation of cybersecurity standards, it only applies to less than 2 % of SMEs, both in ISO and Cyber Essentials.

5. Discussion

The presented research provides a comprehensive perspective on the role of cybersecurity in SMEs and highlights crucial points concerning its nature as a merit-good. While the cybersecurity literature for large enterprises has institutionalized cybersecurity as a business asset, estimating its profitability, investment period, and implications in terms of reputation and social responsibility [16,17]; in the case of SMEs, as we have seen, cybersecurity can be considered a merit-good. This means that the rationale behind this characterization is well-founded, emphasizing how cybersecurity, by protecting critical infrastructures and services, provides broad social benefits. Moreover, we have seen that market failures contribute to the underinvestment in cybersecurity within SMEs. Information asymmetries and the evolving nature of cybersecurity threats result in SMEs often investing less than necessary, creating a gap between actual investment and the socially optimal level. Lastly, the public good characteristics of cybersecurity are eloquently explained, emphasizing its non-rivalrous and non-excludable nature. The discussion successfully connects these characteristics to the need for administrative intervention, leading to the development of standards such as ISO 27,000 and Cyber Essentials.

The research questions posed are logical extensions of the merit-good framework. The RQ1 addresses the information gap and asymmetry regarding cybersecurity in SMEs, acknowledging the myopia and lack of awareness among senior managers. Thus, in line with previous works, our results corroborate previous hypotheses, highlighting the lack of information on cybersecurity in SMEs [7]. This is observed in both the lack of information about potential cyber incidents and their impact. This can result from a dual approach. On the one hand, the literature emphasizes that cybersecurity attacks are increasingly sophisticated and covert, hindering detection by SMEs [36]. Secondly, Fernandez de Arroyabe et al. [1], have highlighted the limited knowledge and

Table 5
Regression analysis cybersecurity management (cluster 1).

Variables	Model 1	Model 2	Model 3	Model 4	Model 5	VIF
Size	.982[c] (.312)	1.027[c] (.327)	.980[c] (.313)	.948[a]8 (.320)	.967[c] (.343)	1.140
Growth	.213[b] (.086)	.147[a] (.093)	.215[b] (.088)	.206[b] (.087)	.168[a] (.094)	1.115
Competencies	−0.166[c] (.039)	−0.149[c] (.040)	−0.165[c] (.041)	−0.169[c] (.039)	−0.135[b] (.043)	1.272
DIGITALIZATION		.655[c] (.179)			.661[c] (182)	1.127
CYBERIMPACT			−0.030 (.349)		−0.370 (.376)	1.537
CYBERINCIDENTS				.154 (.127)	.198 (.151)	1.430
−2 Log Likelihood	281.543	280.665	281.687	297.218	290.858	
Chi-Square	13.372	25.727	13.379	14.719	27.435	
Sig.	.004	.000	.010	.005	<.001	
Cox and Snell	.121	.219	.121	.132	.232	
Nagelkerke	.126	.229	.126	.138	.243	
McFadden	.041	.079	.041	.045	.085	

[a] $p < 0.05$.
[b] $p < 0.01$.
[c] $p < 0.001$.

Table 6
Regression Analysis Cybersecurity control (CLUSTER 2).

Variables	Model 1	Model 2	Model 3	Model 4	Model 5	VIF
Size	.610[a] (.120)	.582[a] (.152)	.934[a] (.194)	1.073[b] (.208)	1.004[b] (.393)	1.128
Growth	.597[a] (.109)	.614[a] (.210)	.576[a] (.212)	.594[b] (.109)	.637[a] (.125)	1.163
Competencies	−0.119[b] (.056)	−0.115[b] (.057)	−0.116[b] (.056)	−0.103[a] (.059)	.122[a] (.066)	1.372
DIGITALIZATION		−0.131 (.270)			−0.199 (.272)	1.360
CYBERIMPACT			.379 (.551)		−0.335 (1.156)	1.927
CYBERINCIDENTS				.348 (.360)	.626 (.774)	1.528
−2 Log Likelihood	174.440	177.761	174.036	174.948	176.438	
Chi-Square	15.600	16.862	17.004	17.478	15.185	
Sig.	.003	.002	.006	.003	.005	
Cox and Snell	.181	.188	.191	.203	.220	
Nagelkerke	.196	.203	.206	.219	.237	
McFadden	.077	.080	.081	.087	.095	

*p < 0.05.
[a] p < 0.01.
[b] p < 0.001.

Table 7
Regression analysis cybersecurity management (cluster 2).

Variables	Model 1	Model 2	Model 3	Model 4	Model 5	VIF
Size	.848[b] (155)	.629[b] (.034)	.911[b] (.112)	.757[b] (.051)	.660[a] (.209)	1.128
Growth	.132[b] (.008)	.115[b] (.005)	.151[a] (.004)	.112[a] (.008)	.194[b] (.005)	1.163
Competencies	−0.187[a] (.032)	−0.189[a] (.055)	−0.180[a] (.048)	−0.140[a] (.038)	−0.118[a] (.053)	1.372
DIGITALIZATION		.335 (.286)			.201 (.379)	1.360
CYBERIMPACT			.797 (.752)		.878 (.628)	1.927
CYBERINCIDENTS				.792 (.427)	.806 (.881)	1.928
−2 Log Likelihood	148.164	146.963	141.677	145.812	142.303	
Chi-Square	12.434	13.635	18.921	16.172	19.681	
Sig.	.001	.001	.003	.002	.009	
Cox and Snell	.071	.104	.237	.171	.254	
Nagelkerke	.090	.132	.299	.215	.321	
McFadden	.047	.070	.172	.119	.186	

*p < 0.05.
[a] p < 0.01.
[b] p < 0.001.

Table 8
Implementation of ISO and Cyber Essentials standard (Cluster 1).

ITEMS	ISO		CYBER ESSENTIALS	
	Frequency	*Per cent*	*Frequency*	*Per cent*
• Yes	16	15.0	20	18.7
• No, and do not intend to do so	30	28.0	25	23.4
• No, but is intending to do so	12	11.2	14	13.1
• No, I am not aware of these certifications	48	44.9	47	43.9
TOTAL	106	99.1	99.1	22.0

Table 9
Implementation of ISO and Cyber Essentials standard (Cluster 2).

ITEMS	ISO		CYBER ESSENTIALS	
	Frequency	*Per cent*	*Frequency*	*Per cent*
• Yes	2	1.5	2	1.5
• No, and do not intend to do so	6	4.5	7	5.3
• No, but is intending to do so	3	2.3	5	3.8
• No, I am not aware of these certifications	18	13.6	15	11.4
TOTAL	29	22.0	29	22.0

involvement of senior managers in SMEs in cybersecurity. For instance, the Cyber Security Breaches Survey (2023) notes a low level of cybersecurity updates provided to senior managers of SMEs. Lastly, senior managers in SMEs do not consider themselves targets of cybersecurity attacks, leading to a lack of concern about cybersecurity information. Moreover, we observe a clear information asymmetry on the part of SMEs. While cybersecurity companies argue that SMEs are targets of attacks [11], our results show a lack of information on the part of SMEs.

Regarding RQ2, which explores the drivers behind the implementation of cybersecurity, our results have shown two differentiated groups. The first group, with a higher level of cybersecurity implementation, is driven by the digitalization of SMEs. Thus, in line with previous works, we see that digitalization has been used as a mechanism for cybersecurity [18,31]. This is the case with cloud computing, where companies store their databases to protect them from potential cybersecurity incidents. Moreover, Fernandez de Arroyabe et al. [1] have found a parallelism between the implementation of cybersecurity and the degree of digitalization, reinforcing previous works that highlight the complementarity of cybersecurity routines and organizational processes and digitalization. Our results extend previous works, highlighting that cybersecurity incidents and cybersecurity impact are not drivers motivating SMEs to implement cybersecurity [1]. On the contrary, the second group of SMEs, with a low level of cybersecurity, does not show any significant driver that encourages the implementation of cybersecurity. Thus, we show that approximately half of the companies have no intention of implementing any cybersecurity measures. This may reinforce previous works on the myopia of cybersecurity in companies and the limited involvement of senior managers in cybersecurity decisions [13]. Therefore, we see that the implementation of cybersecurity in SMEs does not stem from cybersecurity incidents or impact but occurs due to other factors, reinforcing our consideration of cybersecurity in SMEs as a merit commodity.

Regarding RQ3, which aims to understand the implementation of

cybersecurity in SMEs, covering both operational control mechanisms and strategic/organizational measures, we observe that companies with a higher level of cybersecurity and digitalization primarily opt for intensive use of cybersecurity control tools, such as protection methods. Software updates, encryption, firewalls, and malware protection are the most common. These results reinforce previous works on the exploration of protection mechanisms in SMEs [1]. However, we see that in terms of cybersecurity management systems, the extension of these practices is very limited, limited to staff allocation, periodic checks, board discussions, and limited use of cybersecurity policies. Regarding the second cluster, characterized by a low level of implementation of both cybersecurity and digitalization, we see a concerning level of use of protection measures, focusing on software updates and firewalls, with almost no implementation of cybersecurity management systems. Therefore, we observe that another characteristic of merit-goods is verified, such as suboptimal consumption, derived from the lack of information and disinterest of senior managers in SMEs in implementing cybersecurity systems.

Lastly, RQ4 examines the impact of standards on the implementation of cybersecurity in SMEs, recognizing the role of institutions in guiding organizational behaviours. Our results show a lack of effectiveness of standardizations such as Cyber Essentials and ISO 27,000s in the implementation of cybersecurity in SMEs. Thus, in line with previous works, we can consider the adequacy of mimetic and normative measures as mechanisms to foster the implementation of cybersecurity, considering that cybersecurity has characteristics of a merit commodity [37]. While large companies, with a clear economic determination of the role of cybersecurity, may be affected by normative and mimetic measures, we see that this is not effective in a merit-good. In this case, a range of measures, both normative, mimetic, and coercive, should be considered. Thus, we can consider that a merit-good should be considered a public good, and therefore, institutional impulse measures should be developed to mitigate the implementation gap of cybersecurity in SMEs.

The empirical findings of this study highlight the fundamental role of cybersecurity within SMEs, reinforcing its characterization as a merit-good due to its extensive social benefits and the critical gap in its optimal provision. A merit-good is primarily characterized by suboptimal consumption by organizations and individuals, stemming from market failures. The results of RQ1 confirm the existence of market failure, such as the lack and asymmetry of information in cybersecurity, acknowledging the myopia and lack of information in SMEs, which leads to suboptimal implementation of cybersecurity. The lack of optimal implementation is further affirmed by the results of RQ2, which show that both cybersecurity incidents and cybersecurity impact in SMEs do not drive cybersecurity implementation. Additionally, from RQ3, we observe that implementation is more focused on operational control systems rather than management systems, which represents a significant differentiating aspect from large enterprises [1]. A second characteristic of merit-goods is that they are public goods, implying that administrations must encourage investment in cybersecurity in SMEs. Therefore, insufficient investment in cybersecurity, driven by the lack of information and asymmetries, underscores the need for greater administrative intervention to align actual investments with the socially optimal level. The results of RQ4 demonstrate how administrations promote the implementation of cybersecurity in SMEs. From our findings, we outline how the characteristics of cybersecurity as a non-rivalrous and non-excludable good necessitate a stronger institutional framework, suggesting that standards like ISO 27000 and Cyber Essentials, while steps in the right direction, and are insufficient on their own. The elucidation of the study on the disconnect between perceived and actual needs for cybersecurity measures in SMEs, exacerbated by the lack of information and commitment from top management, demands a comprehensive approach that combines normative, mimetic, and coercive measures to foster cybersecurity implementation. Essentially, this research advocates for viewing cybersecurity in SMEs not only as a strategic asset but also as a public good, requiring coordinated efforts to close the implementation gap and ensure a safer digital ecosystem for all stakeholders.

Despite the valuable insights provided by this study, certain limitations must be acknowledged. This study should be corroborated by future research to validate that cybersecurity can be considered a merit good. Future studies should utilize diverse samples across various geographical contexts to enhance the generalizability of the results.

6. Conclusion

In conclusion, this research contributes significantly to the understanding of the role of cybersecurity in SMEs by framing it within the concept of a merit-good. This theoretical contribution sheds light on the distinctive nature of cybersecurity in SMEs, emphasizing its characteristics as a commodity that provides broad social benefits. Unlike large enterprises, where cybersecurity is often treated as a business asset, SMEs face unique challenges and exhibit underinvestment tendencies, making them aptly classified as merit-goods. Moreover, this research advances the discourse on cybersecurity in SMEs, offering a theoretical foundation, practical insights for managers, and guidance for policymakers. Recognizing cybersecurity as a merit-good provides a holistic framework to address the unique challenges faced by SMEs, ultimately contributing to the enhancement of cybersecurity practices in this crucial sector.

As a *theoretical contribution to the field of cybersecurity*, we consider that the merit-good framework applied to cybersecurity in SMEs provides a novel theoretical lens, enriching the discourse in cybersecurity literature. It highlights the societal importance of cybersecurity beyond individual and organizational boundaries. By recognizing the suboptimal consumption of cybersecurity due to information gaps, asymmetries, and a lack of recognition of its broader benefits, this framework captures the nuanced dynamics specific to SMEs. Moreover, highlighting the public good characteristics of cybersecurity reinforces the need for administrative interventions, such as the development of standards, to bridge the implementation gap and ensure the overall security of critical infrastructures.

As *managerial and policy implications*, the findings of this research hold several managerial and policy implications. For SME managers, understanding that cybersecurity is a merit-good necessitates a shift in perspective towards recognizing the broader societal benefits. Awareness campaigns targeting senior managers should emphasize the social responsibility aspect of cybersecurity, addressing the myopia identified in SMEs. Additionally, policies and interventions should focus on providing incentives for SMEs to invest adequately in cybersecurity, considering the non-excludable and non-rivalrous characteristics. Governments and regulatory bodies can play a pivotal role by encouraging the adoption of standards, such as ISO 27,000 and Cyber Essentials, and offering support programs to enhance the cybersecurity position of SMEs.

While this research contributes valuable insights, it is essential to acknowledge its limitations. Firstly, the study primarily draws on existing literature, and future empirical research could provide a more granular understanding of the challenges faced by SMEs in implementing cybersecurity measures. Additionally, the context-specific nature of SMEs implies that the findings may not be universally applicable. The study emphasizes the need for a nuanced approach considering the diverse characteristics of SMEs across industries and regions. Lastly, the rapidly evolving nature of cybersecurity threats implies that the conclusions drawn are subject to change, emphasizing the need for ongoing research to stay abreast of emerging challenges and opportunities.

CRediT authorship contribution statement

Marta F. Arroyabe: Writing – review & editing, Writing – original draft, Supervision, Investigation, Formal analysis, Conceptualization.

Carlos F.A. Arranz: Writing – original draft, Supervision, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Ignacio Fernandez De Arroyabe:** Writing – review & editing, Writing – original draft, Resources, Methodology, Investigation, Formal analysis, Conceptualization. **Juan Carlos Fernandez de Arroyabe:** Writing – review & editing, Writing – original draft, Resources, Methodology, Formal analysis, Data curation, Conceptualization.

Data availability

The data that has been used is confidential.

References

[1] J.C. Fernandez de Arroyabe, M.F. Arroyabe, I. Fernandez, C.F. Arranz, Cybersecurity resilience in SMEs. A machine learning approach, J. Comput. Inf. Syst. (2023) 1–17.

[2] R.F. Babiceanu, R. Seker, Cyber resilience protection for industrial internet of things: a software-defined networking approach, Comput. Ind. 104 (2019) 47–58.

[3] S. Kabanda, M. Tanner, C. Kent, Exploring SME cybersecurity practices in developing countries, J. Organ. Comput. Electron. Commer. 28 (3) (2018) 269–282.

[4] ISO/IEC 27002:2022, Information Security, Cybersecurity and Privacy Protection — Information Security Controls, ISO/IEC, Geneva, 2022.

[5] A. Gilchrist, Industry 4.0: the Industrial Internet of Things, Apress, 2016.

[6] Deloitte, Digitalising SMEs: the role of digitalisation and digital policy in supporting the SME economic recovery. https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/strategy/sea-cons-podcast-fom-epi-9-digitising-movement-goods-transcript.pdf, 2020.

[7] I. Fernandez De Arroyabe, J.C. Fernandez de Arroyabe, The severity and effects of Cyber-breaches in SMEs: a machine learning approach, Enterprise Inf. Syst. 17 (3) (2021) 1942997.

[8] European Commission, Growth - Internal Market, Industry, Entrepreneurship and SMEs, European Commission, 2022. https://ec.europa.eu/growth/smes_en.

[9] M. Mirtsch, J. Kinne, K. Blind, Exploring the adoption of the international information security management system standard ISO/IEC 27001: a web mining-based analysis, IEEE Trans. Eng. Manag. 68 (1) (2020) 87–100.

[10] I.F. Fernandez de Arroyabe, C.F. Arranz, M.F. Arroyabe, J.C.F. de Arroyabe, Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: a UK survey for 2018 and 2019, Comput. Secur. 124 (2023) 102954.

[11] R. Boswell, 60% of European SMEs that are cyber-attacked have to close after six months, Startup Magazine (2023). https://startupsmagazine.co.uk/article-60-european-smes-are-cyber-attacked-have-close-after-six-months.

[12] M. Benz, D. Chatterjee, Calculated risk? A cybersecurity evaluation tool for SMEs, Bus. Horiz. 63 (4) (2020) 531–540.

[13] GOV.UK, Cyber Security Breaches Survey 2023. Department for Science, Innovation and Technology, 2023. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023.

[14] K.R. Choo, The cyber threat landscape: challenges and future research directions, Comput. Secur. 30 (8) (2011) 719–731.

[15] T. Nam, Understanding the gap between perceived threats to and preparedness for cybersecurity, Technol. Soc. 58 (2019) 101122.

[16] M. Lezzi, M. Lazoi, A. Corallo, Cybersecurity for Industry 4.0 in the current literature: a reference framework, Comput. Ind. 103 (2018) 97–110.

[17] ISO/IEC 15408-1:2009, Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 1: Introduction and General Model, ISO/IEC, 2018. https://www.iso.org/standard/50341.html.

[18] A. Corallo, M. Lazoi, M. Lezzi, Cybersecurity in the context of Industry 4.0: a structured classification of critical assets and business impacts, Comput. Ind. 114 (2020) 103165.

[19] N.Y. Conteh, P.J. Schmick, Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks, Int. J. Adv. Comput. Res. 6 (23) (2016) 31–43.

[20] J. Tirole, Market failures and public policy, Am. Econ. Rev. 105 (6) (2015) 1665–1682.

[21] R.O. Zerbe Jr, H.E. McCurdy, The failure of market failure, J. Pol. Anal. Manag.: The Journal of the Association for Public Policy Analysis and Management 18 (4) (1999) 558–578.

[22] M. Kianpour, S.J. Kowalski, H. Øverby, Advancing the concept of cybersecurity as a public good, Simulat. Model. Pract. Theor. 116 (2022) 102493.

[23] M. Taddeo, Is Cybersecurity a Public Good? *Minds And Machines*, vol. 29, 2019, pp. 349–354.

[24] S. Weber, Coercion in cybersecurity: what public health models reveal, Journal of Cybersecurity 3 (3) (2017) 173–183.

[25] W. Ver Eecke, Ethical Dimensions of the Economy: Making Use of Hegel and the Concepts of Public and Merit Goods, Springer Science & Business Media, 2008.

[26] R. Fiorito, T. Kollintzas, Public goods, merit goods, and the relation between private and government consumption, Eur. Econ. Rev. 48 (6) (2004) 1367–1398.

[27] R.A. Alsharida, B.A.S. Al-rimy, M. Al-Emran, A. Zainal, A systematic review of multi perspectives on human cybersecurity behavior, Technol. Soc. (2023) 102258.

[28] R. Al Nafea, M.A. Almaiah, Cyber security threats in the cloud: a literature review, in: 2021 International Conference on Information Technology (ICIT), IEEE, 2021, pp. 779–786.

[29] B.J. Blažič, The cybersecurity labour shortage in Europe: moving to a new concept for education and training, Technol. Soc. 67 (2021) 101769.

[30] K. Macnish, J. Van der Ham, Ethics in cybersecurity research and practice, Technol. Soc. 63 (2020) 101382.

[31] E. Bertino, K.K.R. Choo, D. Georgakopolous, S. Nepal, Internet of things (IoT) smart and secure service delivery, ACM Transaction on Internet Technology 16 (4) (2016) 22–29.

[32] M. Fromhold-Eisebith, P. Marschall, R. Peters, P. Thomes, Torn between digitized future and context dependent past–How implementing 'Industry 4.0'production technologies could transform the German textile industry, Technol. Forecast. Soc. Change 166 (2021) 120620.

[33] K.R. Agbodoh-Falschau, B.H. Ravaonorohanta, Investigating the influence of governance determinants on reporting cybersecurity incidents to police: evidence from Canadian organizations' perspectives, Technol. Soc. 74 (2023) 102309.

[34] D. Horváth, R.Z. Szabó, Driving forces and barriers of Industry 4.0: do multinational and small and medium-sized companies have equal opportunities? Technol. Forecast. Soc. Change 146 (2019) 119–132.

[35] M.J. Sule, M. Zennaro, G. Thomas, Cybersecurity through the lens of digital identity and data protection: issues and trends, Technol. Soc. 67 (2021) 101734.

[36] ENISA, ENISA *Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread And Undetected*, European Union Agency For Cybersecurity, 2020. https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends.

[37] A. Calder, Cyber Essentials: A Pocket Guide, IT Governance Ltd, 2014.

[38] S.S. Hussain, R. Mushtaq, S.A. Rizvi, Impact of top management support on cybersecurity: a case of business organizations in Pakistan, Journal of Information Assurance and Security 11 (1) (2016) 7–18.

[39] R. Von Solms, J. Van Niekerk, From information security to cyber security, Comput. Secur. 38 (2013) 97–102.

[40] M. Bada, A.M. Sasse, J.R. Nurse, Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?, 2015. *ArXiv preprint arXiv:1505.02031*.

[41] P.A. Williams, What cyber security strategies can learn from health promotion, Health Promot. Int. 31 (4) (2016) 755–759.

[42] M. Gale, I. Bongiovanni, S. Slapnicar, Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead, Comput. Secur. 121 (2022) 102840.

[43] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, C. Jerram, Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q), Comput. Secur. 42 (2014) 165–176.

[44] P.M. Podsakoff, S.B. MacKenzie, J.Y. Lee, N.P. Podsakoff, Common method biases in behavioral research: a critical review of the literature and recommended remedies, J. Appl. Psychol. 88 (5) (2003) 879.

[45] T. Masood, P. Sonntag, Industry 4.0: adoption challenges and benefits for SMEs, Comput. Ind. 121 (2020) 103261.

[46] S. Nambisan, K. Lyytinen, Y. Yoo (Eds.), Handbook of Digital Innovation, Edward Elgar Publishing, 2020.

[47] A. Dudek, Silhouette index as clustering evaluation tool, in: *Classification And Data Analysis: Theory And Applications* 28, Springer International Publishing, 2020, pp. 19–33.

[48] A.R. Mamat, F.S. Mohamed, M.A. Mohamed, N.M. Rawi, M.I. Awang, Silhouette index for determining optimal k-means clustering on images in different color models, International Journal of Enginery Technology 7 (2) (2018) 105–109.

[49] R.E. Kass, L. Wasserman, A reference Bayesian test for nested hypotheses and its relationship to the Schwarz criterion, J. Am. Stat. Assoc. 90 (431) (1995) 928–934.

[50] C. Fraley, A.E. Raftery, How many clusters? Which clustering method? Answers via model-based cluster analysis, Comput. J. 41 (8) (1998) 578–588.

[51] World Bank, World Bank SME Finance: Development News, Research, Data, World Bank, 2022. https://www.worldbank.org/en/topic/smefinance.