Computers & Security 141 (2024) 103826

Contents lists available at ScienceDirect

Computers & Security

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

Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives

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:
Cybercrime
SMEs
Cyberspace Theory
Fear
Taxonomy

ABSTRACT

This paper investigates cybercrime in Small and Medium Enterprises (SMEs) using Cyberspace Theory as a theoretical framework for a comprehensive analysis. Cyberspace Theory enables a thorough examination of cybercrime in SMEs, covering motives and consequences of cyber incidents, and identifying existing gaps. The study also delves into SMEs' perception of cybercrime fear, interpreting fear as their concern for cybercrime risk and its potential consequences. Drawing from a robust European Union database comprising 12,863 SMEs across member countries, our research contributes by establishing a taxonomy based on SMEs' perceptions of cybercrime fear. Understanding SMEs' views on cybercrime is crucial for enhancing cybersecurity measures and comprehending the broader economic and social implications of cybercrime.

1. Introduction

In the current digitally-driven landscape, the widespread threat of cybercrime emerges over businesses of all sizes, starting a new era of challenges and vulnerabilities (Babiceanu and Seker, 2019; Choo, 2011). As organizations increasingly rely on interconnected technologies and online platforms to conduct business, the potential impact of cyber incidents develops (Corllo et al., 2020; Deloitte, 2020). Cybercrime encompasses a spectrum of malicious activities, ranging from sophisticated hacking and data breaches to social engineering and ransomware attacks (Fernandez de Arroyabe and Fernandez de Arroyabe, 2023). According to Fox (2024), the annual global cost of cybercrime is projected to reach 9.5 trillion dollars in 2024, with expectations that it will rise to 10.5 trillion dollars in 2025. More in detail, in the healthcare industry, the increase in cyber breaches is surprising, with a 239% rise in large breaches involving hacking over the last four years, leading to an average financial loss of nearly $11 million per breach (Chief Healthcare Executive, 2024). Similarly, the manufacturing sector faces an escalation of cyber threats, constituting 20% of all extortion campaigns globally, with ransomware incidents alone representing 65% of industrial breaches in 2022 (Poireault, 2024). In the finance and insurance sector, exposure to confidential files remains extensive, and financial organizations take an average of 233 days to detect and contain breaches. Furthermore, 74% of cyberattacks compromise clients' data, highlighting the magnitude of the risk. Educational institutions face relentless cyber-attacks: phishing campaigns and vulnerability exploitation account for 29% and 30% of attacks, respectively (Moody, 2024).

Within an era characterized by technological advancement and the extensive influence of digital transformation, small and medium enterprises (SMEs) assume a pivotal role in the economic landscape. These entities serve as focal points for innovation, job creation, and economic expansion, contributing significantly to global economic development, representing approximately 90% of businesses worldwide and accounting for over 50% of global employment (Fernandez de Arroyabe et al., 2023a), However, as SMEs increasingly integrate digital technologies into their operations to reinforce competitiveness, they face an increasing threat: cybercrime. Cybersecurity breaches not only expose the confidentiality, integrity, and availability of sensitive data but also have far-reaching implications for SMEs' operational and financial stability, as well as their reputations (Boswell, 2023). While cybersecurity discourse often revolves around large corporations, Horváth and Szabó (2019) emphasize that SMEs present attractive targets for

[*] Corresponding author.
E-mail address: jcfern@essex.ac.uk (J.C.F. de Arroyabe).

https://doi.org/10.1016/j.cose.2024.103826
Received 20 February 2024; Received in revised form 20 March 2024; Accepted 25 March 2024
Available online 5 April 2024

cybercriminals due to perceived vulnerabilities, resource constraints, and sometimes, inadequate cybersecurity measures. These enterprises encounter unique challenges in addressing cybersecurity, lacking the resources and expertise of larger counterparts to effectively combat cyber threats (Arranz et al., 2024). Despite their size, SMEs are not exempt from cyber-attacks and are increasingly targeted by cybercriminals seeking to exploit system vulnerabilities. Furthermore, SMEs often rely on third-party vendors and partners for various services, introducing additional cybersecurity risks through supply chain vulnerabilities. Kabanda et al. (2018) stress that given the interconnected nature of the contemporary business environment and the evolving tactics of cyber adversaries, cybercrime poses formidable challenges for SMEs.

This study focuses on examining the phenomenon of cybercrime affecting SMEs. We will draw upon a comprehensive European Union database that includes information on 12,000 SMEs from across all EU member states. This research takes place within the context of the European Union, where SMEs play a pivotal role in economic growth, representing over 99% of all businesses, employing 94 million individuals, and contributing to more than half of the total value added by the business sector (World Bank Finance, 2021; Bella et al., 2023). Furthermore, unlike previous research, which primarily employed qualitative approaches or relied on small sample sizes, our utilization of a vast EU database will facilitate the development of well-rounded and widely generalizable conclusions. Secondly, as a theoretical framework, we will employ Cyberspace Theory (Caton, 2012; Adams and Albakajai, 2016). Unlike previous studies using alternative approaches, leading to a diversity of perspectives and inconclusive results regarding the characterization of cybercrime, the use of this theoretical framework allows us to characterize cybercrime in SMEs comprehensively (Cook et al., 2023). This encompasses understanding the motives behind cybercrime, the impact of cyber incidents, and the existing gaps in SMEs. Lastly, unlike prior works that focused on cybersecurity practices and technical issues in SMEs, our analysis centres on the perception of fear of cybercrime within SMEs. We consider fear as the concern SMEs have regarding the risk of cybercrime. In this regard, there is a certain controversy in how SMEs confront cybercrime (Fernandez de Arroyabe et al., 2023a). On one hand, there is a level of naivety amongst SMEs when facing cybercrime, as they may believe they are not likely targets for cyberattacks. This myopic perspective results in low investments in cybersecurity. However, the reality shows that 40% of SMEs experience cyber impacts as a consequence of these cybercrimes (GOV.UK, 2023). Networks are not only filled with targeted attacks, but a high percentage of them are automated and indiscriminate, potentially affecting any company (Benz and Chatterjee, 2020). On the other hand, the perception of fear and concern about cybercrime is, in itself, a harm (Cook et al., 2023; Brands and van Wilsem, 2021). It may lead SMEs to avoid reasonably probable real damages, causing a deterrent in participating in networked economic activities. Therefore, understanding how SMEs perceive the cybercrime threat and the factors influencing these perceptions is a crucial element. This understanding is vital not only for addressing cybersecurity in SMEs but also for comprehending the economic and social implications that cybercrime may bring about.

This paper contributes to the field by applying Cyberspace Theory to analyse the perception and response of SMEs to cybercrime. The analysis focuses on understanding the factors influencing fear in SMEs, concluding in a taxonomy that characterizes different SME profiles. The study not only identifies managerial implications emphasizing robust cybersecurity measures and dynamic risk assessments but also underscores political implications, advocating for policy support, information sharing, regulatory compliance, public awareness, and capacity-building initiatives. Overall, the paper enriches both theoretical and practical perspectives on cybersecurity within the SME sector.

2. Literature review and research framework

2.1. Theoretical framework: cybercrime and cyberspace theory

Cyberspace theory integrates diverse viewpoints and methodologies to examine and comprehend the virtual world of cyberspace (Caton, 2012; Adams and Albakajai, 2016). Its fundamental principle posits cyberspace as a realm distinctly apart from the tangible world. Often described as a virtual or digital space, cyberspace is constituted by a complex network of interconnected computers, servers, and digital devices where information exchange, communication, and digital interactions occur (Adams and Albakajai, 2016). This theory delves into the digital domain's socio-political, cultural, and economic issues (Albakajai et al., 2020). It investigates how people, groups, and entire societies utilize and move through cyberspace, tackling issues like digital identity, privacy concerns, cybersecurity measures, rights within the digital landscape, and the spread of accessible information.

In our research, we adopt the definition of cyberspace as outlined by the United States Department of defense (2008), which describes cyberspace as *a global domain within the information environment constituted by a network of interdependent information technology infrastructures. This includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers*. Furthermore, given that the focus of this paper is on cybercrime, and in alignment with the stance of CISA.gov (2020), our definition of cyberspace expands to include the operators of cyberspace. This extension expands the definition to encompass not just the virtual environment of information but also the interactions amongst individuals, thereby emphasizing the critical role of human elements within the technical infrastructure. It acknowledges the dynamic interplay between technology and its users in the ongoing evolution and characterization of cyberspace.

In this context, cybercrime refers to criminal activities that occur within the digital domain of cyberspace (Papakonstantinou, 2010; Brenner, 2010; Wall, 2007). It involves the use of computers, networks, and digital devices to commit illegal acts, exploit vulnerabilities, and breach security measures for personal gain or malicious purposes. Following Papakonstantinou (2010), a key aspect of cybercrime in cyberspace theory is its disruptive and transformative nature. Unlike traditional forms of crime, cybercrime transcends geographical boundaries and physical constraints, enabling perpetrators to target victims and commit illegal acts worldwide (Brenner, 2010; Walden, 2005). This characteristic of cybercrime challenges traditional notions of jurisdiction, law enforcement, and governance, creating complex legal and regulatory issues in addressing cybercriminal activities. Cybercriminals exploit software vulnerabilities, network weaknesses, and digital infrastructure to conduct a wide range of illegal activities, including hacking, malware distribution, identity theft, fraud, phishing, and cyber espionage (Wall, 2007). These activities not only pose significant risks to individuals, organizations, and governments but also have far-reaching implications for trust, privacy, and security in cyberspace. In this study, cybercrime is defined as a collection of illicit activities that utilize digital technologies, networks, and computer systems as tools, targets, or mediums for unlawful actions.

Understanding cybercrime within the framework of cyberspace theory entails examining its various dimensions, encompassing its effects on individuals, societies, and the broader digital ecosystem (Papakonstantinou, 2010; Wall, 2007). Applying this theory to cybercrime in SMEs requires not only analysing the motives driving cybercriminal behaviour but also scrutinizing the practices and operations within these organizations, as well as the factors that render them susceptible to cyber threats. Cybercriminals can range from individual hackers and organized criminal groups to state-sponsored actors engaged in cyberwarfare (Brenner, 2010). Cybercrime operates on a global scale, transcending geographical borders (Walden, 2005). Criminals can launch attacks from one part of the world and target victims in another. The international nature of cybercrime poses challenges for regulatory and law enforcement agencies in terms of jurisdiction and coordination (Walden, 2005; Wall, 2007).

Cybercriminals target individuals, businesses, governments, and critical infrastructure. Thus, cybercriminals find various motivations for cybercrime. In the literature, numerous reasons are identified for which cybercriminals may exploit vulnerabilities in companies (ENISA, 2020). These reasons include economic gains, espionage, data theft, extortion, and more. No sector is immune to cyber threats, ranging from opportunistic and indiscriminate attacks to sophisticated and highly selective campaigns against specific entities (Fernandez de Arroyabe et al., 2023b). These crimes may involve unauthorized access, disruption, or manipulation of information and digital assets. As seen in Table 1, the scope of cybercrime extends across a broad spectrum of activities, including hacking, identity theft, online fraud, malware attacks, denial-of-service (DoS) attacks, phishing, and the distribution of malicious software, for example (ENISA, 2020).

Regarding the mechanism employed by cybercriminals to execute cybercrime, they leverage the interconnected nature of businesses and the increasing volume of activities that SMEs are conducting online, thereby intensifying their exposure to cybersecurity incidents. Consequently, businesses find themselves susceptible to cyberattacks, which are continuously growing in sophistication and diversifying, making it challenging for companies to safeguard their systems (Fernández De Arroyabe and Fernández de Arroyabe, 2023; Conteh and Schmick, 2016). Cybersecurity attacks can manifest in various ways, contingent on the attacker's objectives, the execution method, and the identity of the perpetrator. The literature identifies different types of adversaries employing diverse techniques, including phishing, malware or web attacks, and the exploitation of vulnerabilities stemming from mismanagement of computer systems within organizations. ENISA has categorized several types of cyber-attacks (ENISA, 2020), with malware representing 30% of all cyberattacks. Other attacks encompass assaults on websites and domains to steal personal information and banking data, as well as phishing attempts seeking identity impersonation and malware implementation. In addition to external threats, internal personnel can also instigate security breaches, either intentionally or inadvertently. ENISA (2020) underscores the significance of such insider threats, indicating that 77% of data leaks in companies result from incidents related to insider information. Table 2 presented here offers an overview of major cyberattacks, recognizing that it is not exhaustive, as cybercriminals continually refine and diversify their tactics, and new attack methods may emerge over time. It is crucial to acknowledge that cybersecurity threats evolve constantly, and novel attack methods may emerge over time.

Table 1
Cybercrime targets companies (source ENISA, 2020).

Target	Description
Financial Gain	• Cybercriminals may attempt to steal sensitive financial information, such as credit card details or banking information, to make monetary gains.
Corporate Espionage	• Competitors companies or nation-states may engage in cyberattacks to steal valuable intellectual property, trade secrets, or research and development data.
Disruption of Services:	• Some cyberattacks are carried out with the sole purpose of disrupting a company's normal operations, causing financial loss and reputational damage.
Data Violation	• Cybercriminals can target companies to gain access to personal or sensitive information, which they can then sell on the dark web or use for identity theft.
Political Motivations	• Nation-states or politically motivated groups may carry out cyberattacks to achieve geopolitical objectives, gather intelligence, or disrupt the operations of rival nations.
Internal or Insider Threats	• Insiders, whether discontented employees or those with malicious intent, can intentionally or unintentionally compromise a company's security.
Extortion	• Cybercriminals may threaten to reveal sensitive or embarrassing information unless the company pays a ransom or meets specific demands.

Finally, cybercriminals exploit vulnerabilities within SMEs to engage in activities with the potential for financial gains, compromise of data, or disruption of digital operations. These criminals employ a diverse array of methods, encompassing the exploitation of software vulnerabilities, social engineering, phishing emails, ransomware attacks, and the utilization of botnets (ENISA, 2020; Fernandez de Arroyabe et al., 2023a). The ever-evolving nature of technology creates fertile ground for the development of novel attack-vectors. Additionally, Choo (2011) emphasizes internal vulnerabilities within a company, which pertain to weaknesses or gaps in the organization's internal systems, processes, or practices that could be exploited by malicious actors. These vulnerabilities may exist at various levels, including technology, personnel, and procedures. Table 3 shows some common internal vulnerabilities of the companies (ENISA, 2020).

2.2. SME and cybercrime: research questions

As previously mentioned, SMEs play a significant social and economic role in society, with estimates suggesting that more than 90% of businesses in Europe fall into this category (Bella et al., 2023). In terms of their contribution to employment and GDP, SMEs account for approximately 40% and 60%, respectively. However, despite their importance, SMEs are not immune to the threat of cybercrime. In fact, it has been observed that over 40% of SMEs have experienced cyberattacks. Additionally, research indicates that 75% of SMEs would struggle to continue operating if they were targeted by ransomware attacks. Furthermore, nearly 40% of small businesses have reported significant data loss following a cyberattack. Alarmingly, it has been found that 51% of small businesses affected by ransomware opt to pay the ransom (Rahmonbek, 2024). These statistics confirm that SMEs are vulnerable to cybercrime and its detrimental effects.

However, the perception of cybercrime in terms of fear is contradictory. Firstly, a subset of studies emphasizes that senior managers in SMEs consider themselves not inclined to cybercrime, arguing that such attacks are primarily directed at large companies due to the perceived limited returns on targeting SMEs (see for example, Fernandez de Arroyabe et al., 2023a). Consequently, cybercrime does not generate concern within these SMEs. Following previous literature, this translates into a lack of involvement by senior managers in IT security issues, as well as poor communication between IT departments and SME leadership (GOV.UK, 2023). For instance, in the context of a cyber breach, approximately 50% of SMEs exhibit limited investment in cybersecurity, and the existence of cyberattacks and incidents is not ascertained (GOV.UK, 2023). Similarly, it is noted that 40% of senior managers in SMEs either do not receive information about cybercrime or receive it only once a year. Secondly, another set of studies indicates that certain SMEs invest in cybersecurity as they expand their online activities, driven by a perception of fear and concern regarding cybercrime. Lastly, empirical evidence suggests that certain SMEs curtail their online activities to avoid exposure to networks and the potential dangers of cybercrime, resulting in a subsequent decline in economic activity. Therefore, in light of these contradictory perceptions of cybercrime within SMEs, our primary research question seeks to investigate the fear in SMEs concerning cybercrime:

Research question (RQ1). *How do SMEs perceive cybercrime in terms of fear?*

The second question aims to investigate the factors influencing the existence of fear regarding cybercrime. Thus, in addition to considering the characteristics of SMEs, we will focus on three factors: the level of digitization, previous experiences of cybercrime, and the impact suffered by the SME as a result of attacks.

Firstly, we will analyse how the activities conducted on the network impact the fear associated with cybercrime. In this regard, the digitalization of businesses is primarily based on the adoption of emerging

Table 2
The main cyberattacks the companies (source ENISA, 2020).

- **Malware**: Short for malicious software, malware includes a variety of harmful software such as viruses, worms, trojan horses, ransomware, and spyware. Malware is designed to disrupt, damage, or gain unauthorized access to computer systems.
- **Phishing:** Phishing attacks involve tricking individuals into providing sensitive information, such as usernames, passwords, and credit card details, by posing as a trustworthy entity. Phishing is often carried out through emails, messages, or websites that mimic legitimate sources.
- **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks:** These attacks aim to overwhelm a system, network, or website with excessive traffic, rendering it unavailable to users. In a DDoS attack, multiple compromised computers are used to generate the traffic, making it more difficult to mitigate.
- **Man-in-the-Middle (MitM) Attacks:** In MitM attacks, an attacker intercepts and potentially alters the communication between two parties without their knowledge. This can occur in various forms, including eavesdropping on Wi-Fi networks or intercepting data between a user and a website.
- **SQL Injection:** This type of attack targets the vulnerabilities in a website's database by injecting malicious SQL code. Successful SQL injections can allow attackers to manipulate or retrieve data from the database.
- **Cross-Site Scripting (XSS):** XSS attacks involve injecting malicious scripts into websites that are viewed by other users. These scripts can then execute in the context of the user's browser, potentially stealing information or performing actions on behalf of the user without their consent.
- **Ransomware**: Ransomware is a type of malware that encrypts a user's files and demands payment (usually in cryptocurrency) in exchange for the decryption key. It can severely impact individuals and organizations, denying access to critical data until the ransom is paid.
- **Zero-Day Exploits**: Zero-day exploits target vulnerabilities in software or hardware that are unknown to the vendor or not yet patched. Attackers exploit these vulnerabilities before they are discovered or fixed.

Table 3
The main vulnerabilities in the companies (source ENISA, 2020).

Vulnerability	***Actions***
Weak Passwords	• *Weak or easily guessable passwords can provide unauthorized access to sensitive systems or data.*
Insufficient Access Controls	• *Inadequate access controls may lead to employees having more access privileges than necessary for their roles.*
Outdated Software and Systems	• *Failure to regularly update and patch software and systems leaves them vulnerable to exploitation by known vulnerabilities.*
Lack of Security Training	• Employees who are not adequately trained in cybersecurity awareness may fall victim to social engineering attacks.
Insider Threats	• *Employees with malicious intent can pose a significant threat.*
Inadequate Network Security	• *Poorly secured wireless networks can be exploited by attackers to gain unauthorized access to the organization's internal network.*
Unrestricted Use of Removable Media	• *Allowing unrestricted use of USB drives or other removable media can lead to data leakage.*
Insecure Configuration Settings	• *Failure to change default settings on hardware, software, or network devices may expose vulnerabilities that attackers can exploit.*
Inadequate Incident Response Planning	• *The lack of a well-defined incident response plan can result in delays in identifying, containing, and mitigating the impact of a security incident.*
Poor Physical Security	• *Insufficient controls to prevent unauthorized personnel from accessing physical facilities or critical infrastructure can lead to security breaches.*
Data Storage and Transmission Insecurity	• *Storing or transmitting sensitive data without encryption increases the risk of data interception or unauthorized access.*
Vendor and Third-Party Risks	• *Using third-party services or products without thoroughly vetting their security practices can introduce vulnerabilities into the organization's environment.*

technologies and the intensive use of networks (Masood and Sonntag, 2020; Dabrowska et al., 2022). While digitalization has a significant impact on innovation and business productivity (Dalenogare et al., 2018; Nambisan et al., 2020; Manesh et al., 2020) and involves the interconnection of businesses, enabling the permeability of social networks and facilitating access to information or new markets (Moeuf et al., 2019; Vial, 2021), it also poses a greater exposure of companies to cybersecurity incidents resulting from vulnerabilities in the use of information technologies, presenting security challenges (Arroyabe et al., 2024; Fernández de Arroyabe et al., 2023b; Benz and Chatterjee, 2020; Lezzi et al., 2018). Thus, for classic attacks like spyware, malware, denial-of-service (DoS), ransomware, or phishing, the interconnected devices of SMEs can serve as potential entry points for cybersecurity incidents (Choo, 2011; Fernández de Arroyabe and Fernández de Arroyabe, 2023). The connected nature of networks means that every poorly protected device connected online potentially impacts the security and resilience of the company (Corallo et al., 2020; Kabanda et al., 2018). Therefore, it is expected that the activities on the internet of SMEs may influence the fear and concern regarding cybercrime.

Secondly, it is expected that previous experiences will impact the fear towards cybercrime. The occurrence of prior attacks should increase the perception of cybercrime in SMEs for various reasons. Firstly, SMEs with limited cybersecurity resources may lack dedicated personnel or comprehensive cybersecurity measures, making them more vulnerable to attacks (Arroyabe et al., 2024). The fear of being ill-prepared to defend against sophisticated cyber threats can be a source of concern for these businesses. Secondly, many SMEs heavily rely on digital operations for various aspects of their business, including communication, transactions, and interactions with customers (Horváth and Szabó, 2019; Masood and Sonntag, 2020). A successful cyberattack can disrupt these operations, instilling fear about potential impacts on daily business activities. Due to concerns about data loss and privacy, SMEs often handle confidential business and customer data. The fear of losing this data due to a cyberattack not only has financial implications but also raises concerns about privacy and compliance with data protection regulations. Thirdly, SMEs may be part of larger supply chains (Fernandez de Arroyabe et al., 2023). Cyberattacks targeting suppliers or partners can have a cascading effect on SMEs, generating fears about the security and resilience of the entire business ecosystem. Lastly, in some cases, SMEs may have limited awareness of cybersecurity best practices and the evolving threat landscape (Kabanda et al., 2028; Bertino et al., 2016). Fear of the unknown, coupled with a lack of knowledge about potential cyber risks, can contribute to heightened concerns. Therefore, it is expected that SMEs' previous experiences with cybercrime may affect the fear and concern regarding cybercrime.

Finally, not only can experiences affect SMEs' perception of cybercrime, but also being the target of attacks, with the consequent impact on SMEs, should influence the perception of cybercrime. Cyberattacks can significantly impact the fear of SMEs for various reasons (ENISA, 2020). Firstly, the financial impact of a cyberattack, including costs related to remediation, potential legal actions, and loss of business, can be more severe for SMEs. This financial strain can induce fear and anxiety about the business's sustainability. Secondly, SMEs often heavily depend on their reputation within their local communities or market niches; a cyberattack causing data breaches or service interruptions can damage the trust that customers, partners, and stakeholders have in the SME. The fear of reputation damage can be a major concern.

Therefore, we believe that both the level of activities on the internet, previous experiences with cybercrime, and the economic and social impact of cyberattacks can influence SMEs' perception in terms of fear. As a result, we pose the following research question:

RQ2. *How do the activities on the internet, previous experiences, and the* *impact of cyber incidents affect the existence of fear regarding cybercrime in SMEs?*

3. Methodology

3.1. Database

To empirically explore the research questions, we use the database from Eurostat, Flash Eurobarometer No. 496, which is conducted for the European Commission (Eurostat, 2022). This specific survey covers cybercrime, cyber incidents, and digitalisation in SMEs, with a sample of 12,863 SMEs. The fieldwork was conducted between November and December 2021. Interviews were conducted by phone in their respective national languages. The geographical scope of the database includes the 27 countries of the EU. In Tables 4, 5 and 6, we see the distribution of the sample by geographical area, sector and size.

3.2. Measures

The first variable in our research model is the online activities conducted by SMEs. The question posed is, "Which of the following does your company currently have or use?" The question includes the following multi-item options: i) An online bank account; ii) An online ordering and payment service for customers; iii) Online ordering or payment systems of suppliers, consultants, or other business partners; iv) A website for your business; v) Web-based applications for payroll processing, e-signature, etc.; vi) Cloud computing or storage; vii) Internet-connected 'smart' devices; viii) A company intranet; and ix) An internet-based video or voice calling service. To measure the degree of penetration of internet activities in SMEs, we created the variable *activities,* constructed as a cumulative index of nine types of activities.

The second measure is the fear of cybercrime. The question asks: "When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks?" Similar to the previous measure, the questionnaire includes a multi-item question: i) Viruses, spyware, or malware (excluding ransomware); ii) Denial of service attacks; iii) Hacking (or attempts to hack) online bank accounts; iv) Phishing, account takeover, or impersonation attacks; v) Ransomware; vi) Unauthorized accessing of files or networks; vii) Unauthorized listening into video conferences or instant messages; and viii) Any other breaches or attacks. The measurement scale is ordinal, with 1 indicating "very concerned," 2 "somewhat concerned," and 3 "not at all concerned." Similar to the previous variable, the variable *fear* was constructed as a cumulative index of eight types of concerns.

Table 4
Geographical distribution of the sample.

Country	Frequency	%
FR - France	501	3.9
BE - Belgium	502	3.9
NL - The Netherlands	528	4.1
DE - Germany	501	3.9
IT - Italy	505	3.9
LU - Luxembourg	253	2.0
DK - Denmark	510	4.0
IE - Ireland	507	3.9
GR - Greece	502	3.9
ES -Spain	505	3.9
PT - Portugal	511	4.0
FI - Finland	502	3.9
SE - Sweden	500	3.9
AT - Austria	503	3.9
CY - Cyprus (Republic)	251	2.0
CZ - Czech Republic	504	3.9
EE - Estonia	503	3.9
HU - Hungary	501	3.9
LV - Latvia	500	3.9
LT - Lithuania	504	3.9
MT - Malta	252	2.0
PL - Poland	504	3.9
SK - Slovakia	500	3.9
SI - Slovenia	500	3.9
BG - Bulgaria	511	4.0
RO - Romania	502	3.9
HR - Croatia	501	3.9
Total	**12,863**	**100.0**

Table 5
Sector of Activity (NACE) –Sections grouped.

Sector	Frequency	%
Manufacturing (C)	2094	16.3
Retail (G)	3925	30.5
Services (H/I/J/K/L/M/N/P/Q/R)	4985	38.8
Industry (B/D/E/F)	1859	14.5
Total	**12,863**	**100.0**

Table 6
Number of employees.

Employees	Frequency	%
<10 employees	6699	52.1
10 to 49 employees	3934	30.6
50 to 249 employees	2230	17.3
Total	**12,863**	**100.0**

The third group of measures includes variables that refer to the experience with cybercrime. The variables are measured using the question: "Regarding the experience with cyber incidents, how was this attack carried out?" Similar to the previous measures, the questionnaire employs a multi-item question: i) Exploiting software, hardware, or network vulnerabilities; ii) Password cracking; iii) Identity theft; iv) Scams and fraud; v) Malicious software; vi) Denial of service (false traffic to overwhelm a website or network); and vii) Disruption or defacing of web presence. Consistent with previous variables, the variable *experience* was constructed as a cumulative index of seven previous experiences.

Finally, the last variable refers to the impact of cybercrime on SMEs. The question posed in the questionnaire is: "Still thinking about the serious incidents, how was your business impacted?" As in previous variables, the question is multi-item: i) Loss of revenue; ii) Loss of suppliers, customers, or partners; iii) Repair or recovery costs; iv) Ransom money; v) Prevented the use of resources or services; vi) Prevented employees from carrying out day-to-day work; vii) Additional time required to respond to the cybercrime incident(s); viii) Damage to the reputation of the company; and ix) Discouraged us from carrying out an activity that was planned. We have also created a new variable, *impact*, as a result of the cumulative index of impacts.

Additionally, we have controlled our analysis with a series of control variables. These are:

The first control variable is the size, which is measured on a scale of 1 to 3, where 1 represents microenterprises (1 to 9 employees), 2 represents small enterprises (10 to 49 employees), and 3 represents medium-sized enterprises (50 to 249 employees).

The second control variable is the age of the company. We used a Likert scale, where respondents were asked, "How long has your company been in business?" The options include 1 for a company with an age of less than 1 year, 2 for a company with an age between 1 and 5 years, 3 for a company with an age between 6 and 10 years, and 4 for a company with an age of more than 10 years.

The third control variable is the revenue of the company. The question included in the questionnaire is: "What was your company's total turnover in 2020?" The response follows a Likert scale, where 1 represents SMEs with a revenue of less than 25,000 euros, 2 represents more than 25,000 to 50,000 euros, 3 represents more than 50,000 to

100,000 euros, 4 represents more than 100,000 to 250,000 euros, 5 represents more than 250,000 to 500,000 euros, 6 represents more than 500,000 to 2 million euros, 7 represents more than 2 to 10 million euros, 8 represents more than 10 to 50 million euros, and 9 represents more than 50 million euros.

The next control variable is the training received in the SME on cybercrime. The question included in the questionnaire is: "In the last 12 months, has your company provided employees with any training or awareness raising about the risks of cybercrime?"

Finally, we have included a question about the ownership of IT devices in the company or if they are personal devices used by employees for their activities. The question posed is: "Do employees in your company use personally-owned devices such as smartphones, tablets, laptops, or desktop computers to carry out regular business-related activities? This includes devices that are subsidized by your company."

4. Analysis and results

We first checked the robustness of the survey and the results. 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. (2003). The analysis has identified nine distinct constructs that collectively account for 57.94% of the variance. The first factor accounts for 13.30% 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 analysing the research questions, we conducted a descriptive analysis of our results, evaluating both the internet activities of SMEs and their previous experience with cybercrime, as well as its impact in economic and social terms. In Table 7, we present the results of the activities carried out by the companies on the internet. Overall, we observe that basic activities such as having an online bank account (81.8%), having a website (74.6%), and having a connected smart device (64.9%) are the most common amongst SMEs. The remaining activities, such as payment systems, cloud storage, or the use of an intranet, example, are utilized by less than 50% of the companies in the sample. Going deeper into the analysis of activities conducted on the internet, Table 8 shows the cumulative distribution of these activities. From the results, we can note that the highest percentage of cumulative activities in a company corresponds to 4 (16.3%) or five activities (15.7%), and to a lesser extent, some companies engage in 3 or six activities on the Internet.

In Tables 9 and 10, we present the results of SMEs' experience with cybercrime and the impact suffered by these companies. Overall, we observe that in both tables, the response is low, being less than 10% of SMEs, except for attacks on software, hardware, and network vulnerabilities, which are close to 25% of the companies. Regarding the impact of cybercrime on SMEs, we see a diversity of damages, including economic aspects such as costs, operational repair, or theft. We also observe other types of damages such as loss of reputation and acting as a deterrent to potential activities.

Table 7
Activities in internet develops for the SMEs.

Activities	N	%
An online bank account	10,416	81.8
An online ordering and payment service for customers	4687	36.4
Online ordering or payment systems of suppliers, consultants or other business partners	5546	43.1
A website for your business	9597	74.6
Web-based applications for payroll processing, e-signature etc.	6394	49.7
Cloud computing or storage	5883	45.7
Internet-connected 'smart' devices	8347	64.9
A company intranet	4572	35.5
An internet-based video or voice calling service	5164	40.1

Table 8
Distribution of accumulative activities on the Internet of SMEs.

Value	Frequency	%
.00	325	2.5
1.00	782	6.1
2.00	1146	8.9
3.00	1681	13.1
4.00	2099	16.3
5.00	2017	15.7
6.00	1816	14.1
7.00	1396	10.9
8.00	1069	8.3
9.00	532	4.1
Total	**12,863**	**100.0**

Table 9
Experience in cybercrime in SMEs.

Experiences	Frequency	%
Exploiting software, hardware, or network vulnerabilities	830	6.5
Password cracking	672	5.2
Identity theft	578	4.5
Scams and fraud	1143	8.9
Malicious software	1151	8.9
Denial of service (false traffic to overwhelm website or network)	504	3.9
Disruption or defacing of web presence	457	3.7

Table 10
Impact of cybercrime on the SMEs.

Impact	Frequency	%
Loss of revenue	476	3.7
Loss of suppliers, customers, or partners	240	1.9
Repair or recovery costs	993	7.7
Ransom money	232	1.8
Prevented the use of resources or services	871	6.8
Prevented employees from carrying out day-to-day work	976	7.6
Additional time required to respond to the cybercrime incident (s)	1507	11.7
Damage to the reputation of the company	325	2.5
Discouraged us from carrying out an activity that was planned	553	4.3

Regarding the analysis of RQ1, which focuses on the existence of fear about cybercrime in SMEs, Table 11 presents the results of fear about potential cybercrime. This table examines the diverse typology of cybercrime used by cyber attackers and, on the other hand, the degree of concern. Overall, we observe fear or concern in more than 75% of SMEs, indicated by the fact that in the majority of cybercrime cases, the level of unconcern is less than 25%. We also observe a fairly balanced distribution of the types of cybercrime used, indicating how cybercriminals are diversifying their cybercrime tactics.

Regarding RQ2, which investigates how the level of internet activities, experience, or the impact of cybercrime affects the fear or concern of SMEs, Tables 12 and 13 present the results of the regression analyses. In Model 4 of Table 12, it is evident that previous experiences ($\beta=-0.203$; $p < .001$), impact ($\beta=-0.150$; $p < .001$), and the degree of internet activities ($\beta=0.046$; $p < .005$) undertaken by SMEs have a positive impact on the fear of cybercrime in SMEs. Table 12 displays the marginal effects of each independent variable. Overall, we observe that all three functions are monotonically increasing, indicating a growing effect on the dependant variable as the independent variable increases. However, we note that the trajectory of the variable differs across the range of the variables. While the level of internet activities has a complete range across the variable, experiences and impact variables have a limited range within the lower values of the variable. In terms of the robustness of the regression models, we ruled out the existence of collinearity between independent variables, as evidenced by the

Table 11
Level of fear about cybercrime.

Typology of fear	Very concerned		Somewhat		Not at all	
	Frequency	%	Frequency	%	Frequency	%
Viruses, spyware or malware (excluding ransomware)	3466	26.9	5906	45.9	3255	25.3
Denial of service attacks	5338	41.5	4918	38.2	1889	14.7
Hacking (or attempts to hack) online bank accounts	4383	34.1	4945	38.4	3358	26.1
Phishing, account takeover or impersonation attacks	3837	29.8	5584	43.4	3245	25.2
Ransomware	4843	37.7	4854	37.7	2455	19.1
Unauthorised accessing of files or networks	4419	34.4	5588	43.4	2653	20.6
Unauthorised listening to video conferences or instant messages	7081	55.0	3845	29.9	1548	12.0
Any other breaches or attacks	4325	33.6	5900	45.9	2200	17.1

Table 12
Regression analysis of fear.

Variables	Model 1		Model 2		Model 3		Model 4		Model 4		VIF
	Estimate	Error	Estimate	Error	Estimate	Error	Estimate	Error	Estimate	Error	
SIZE	.193***	.025	.161***	.025	.149***	.044	.102*	.044	.139**	.044	1.360
SENIORITY	.082**	.025	.079**	.025	.118**	.047	.119*	.047	.131**	.047	1.060
REVENUE	−0.029***	.007	−0.033***	.007	−0.027*	.003	−0.025**	.003	−0.020**	.003	1.338
TRAINING	.000**	.000	.000**	.000	.000*	.000*	.000	.000	.000**	.000	1.004
DIGITALISATION			.054***	.008					.046**	.015	1.101
EXPERIENCE					.287***	.027			.203***	.029	1.232
IMPACT							.196***	.017	.150***	.019	1.239
−2 Log Likelihood	11,946.740		23,240.781		8830.028		9687.224		16,781.282		
Chi-Square	95.970		141.182		135.361		149.040		204.099		
Sig.	.000		.000		/000		.000		.000		
Cox and Snell	.009		.013		.040		.044		.059		
Nagelkerke	.009		.013		.040		.044		.060		
McFadden	.002		.002		.007		.008		.011		

Variance Inflation Factor (VIF) being less than 2 for all variables. Similarly, we addressed the issue of autocorrelation bias in residuals with the dependant variable using the Durbin-Watson test.

Once we determined how experience, impact, and the level of internet activities affect fear of cybercrime, we conducted an exploratory analysis to classify SMEs into different groups based on the perception of fear. The objective was to obtain a taxonomy of cybercrime and fear. Using the K-mean Cluster as a statistical model (Dudek, 2020; Mamat et al., 2018), we proceeded in two stages. First, the input variables for K-means were the degree of fear or concern and the activities carried out on the internet. Second, we selected the most robust solution using Silhouette analysis (Dudek, 2020; Mamat et al., 2018). This analysis allows us to determine the robustness of the cluster solution, the cohesion of each cluster, and the separation of groups. The silhouette index takes values in the range [−1, 1], with values closer to 1 indicating a more solid solution. After obtaining the Silhouette index, the four-cluster solution has a higher Silhouette value (0.67). Additionally, we conducted a complementary analysis using the Bayesian Schwarz criterion (Kass, 1995; Fraley and Raftery, 2002), and the results confirm that the three-cluster solution is the most robust in terms of cohesion and separation.

The results of the K-means cluster analysis show that SMEs are grouped into four clusters. Furthermore, we conducted a robustness check of the analysis through ANOVA, and the results show a significant difference in the degree of fear and activities conducted on the internet based on the SMEs' membership in each cluster. Tables 14, 15 and 16 display the ANOVA analysis, the number of companies each cluster encompasses, and the main values of each cluster.

In Fig. 1, we present the mean values of the variables fear and internet activities based on SMEs' membership in each cluster. In more detail, we observe that Cluster 4 has a higher level of fear than all the clusters, followed by Cluster 3 and then Cluster 1, with the lowest level of fear in Cluster 2. We also display the level of activities conducted on the internet, noting that the lowest value corresponds to Cluster 3, with a similar level in the other three clusters. On the other hand, in Fig. 2, we see the mean values of experience and the impact of cybercrime on SMEs based on each cluster. Cluster 2 has the lowest mean values, while Cluster 4 has the highest values for impact and experience. Furthermore, Clusters 1 and 3 have mean values for impact and experience with cybercrime.

To control the results of the cluster analysis, we show in Figs. 3 and 4 the mean values of control variables (size, turnover, seniority, sector, and country), classified by cluster, using them as variables. Overall, we observe similar characteristics in the four clusters, with a slight variation in the turnover of the companies. In the case of Cluster 3, we see a slight difference compared to the other clusters. To clarify this result, we conducted an ANOVA analysis, using turnover as the variable and the cluster of belonging as a control variable, and found no significant differences between clusters, ruling out the existence of bias.

Lastly, Fig. 5 presents the average results of actions undertaken by SMEs to manage cybersecurity and cybercrime. Variables such as training conducted by SMEs in the last 12 months on the risks of cybercrime are shown, and the second variable indicates whether SMEs use employees' IT devices. We observe significant variability in training about the risks of cybercrime amongst clusters, with Cluster 2 being the one that has intensively engaged in training activities within the SME. Moreover, we see that this same cluster is the one that most extensively utilizes employees' devices compared to the other clusters. However, Cluster 4 is characterized by the lowest level of training and the use of personal devices in internet activities.

5. Discussion

The application of Cyberspace Theory to cybercrime in SMEs has enabled us to establish a framework for characterizing cybercrime. In contrast to earlier studies that focused either on cyberattacks or cybersecurity measures (see for example, Fernandez de Arroyabe et al., 2023b), the application of Cyberspace Theory has enabled us not only to examine the motives and objectives behind the existence of cybercrime but also to scrutinize the routines and activities within these

Table 13
Regression analysis of marginal values.

Variables	Model 1	Model 2	Model 3	Model 4	Model 4	Model 5
	Estimate	Error	Estimate	Error	Estimate	Error
SIZE	.165***	.025	.146**	.044	.093*	.044
ANTIGUEDAD	.076**	.025	.115*	.047	.123**	.047
REVENUE	−0.033***	.007	−0.026*	.013	−0.024*	.013
TRAINING	.000**	.000	.000**	.000	.000**	.000
[DIGITALISATION=0.00]	−0.758***	.137				
[DIGITALISATION=1.00]	−0.423***	.106				
[DIGITALISATION=2.00]	−0.418**	.099				
[DIGITALISATION=3.00]	−0.237**	.093				
[DIGITALISATION=4.00]	−0.151*	.090				
[DIGITALISATION=5.00]	−0.132*	.090				
[DIGITALISATION=6.00]	−0.140*	.090				
[DIGITALISATION=7.00]	−0.120	.093				
[DIGITALISATION=8.00]	−0.055	.096				
[DIGITALISATION=9.00]	0^{a}	.				
[EXPERIENCE=0.00]			−1.554***	.508		
[EXPERIENCE=1.00]			−1.156***	.505		
[EXPERIENCE=2.00]			−0.958**	.507		
[EXPERIENCE=3.00]			−0.592	.513		
[EXPERIENCE=4.00]			−0.196	.532		
[EXPERIENCE=5.00]			−0.155	.576		
[EXPERIENCE=6.00]			.047	.630		
[EXPERIENCE=7.00]			0^{a}	.		
[IMPACT=0.00]					−1.743***	.619
[IMPACT=1.00]					−1.255***	.620
[IMPACT=2.00]					−1.133**	.621
[IMPACT=3.00]					−1.119*	.624
[IMPACT=4.00]					−0.826	.627
[IMPACT=5.00]					−0.665	.635
[IMPACT=6.00]					−0.466	.647
[IMPACT=7.00]					−0.541	.671
[IMPACT=8.00]					−0.561	.846
[IMPACT=9.00]					0^{a}	.
−2 Log Likelihood	3224.401		8825.465		9669.907	
Chi-Square	157.562		139.924		166.358	
Sig.	.000		.000		.000	
Cox and Snell	.014		.041		.049	
Nagelkerke	.014		.041		.049	
McFadden	.003		.008		.009	

Table 14
ANOVA analysis.

Variables	Sum of Squares	Mean Square	F	Sig.
ACTIVITIES	5162.531 4,922,2.2,38 5,438,4.7,69	1720.844 4.535	379.498	.000
FEAR	190,163.223 3,592,9.9,22 22,609,3.1,46	63,387.741 3.310	19,150.443	.000

Table 15
Distribution of the number of employees for clusters.

Cluster	Frequency	%
1	5325	41.4
2	3638	28.3
3	785	6.1
4	1111	8.6
Missing	2004	15.6
Total	**12,863**	**100.0**

organizations, as well as the factors contributing to their vulnerability to cyber threats. The application of Cyberspace Theory to cybercrime in SMEs facilitates a comprehensive characterization of cybercriminals and cybercrimes (Cook et al., 2023; Choi et al., 2021). Specifically, our findings demonstrate that cybercriminals employ numerous methods through which attackers can exploit vulnerabilities in companies. Consistent with prior research (ENISA, 2020; Fernandez de Arroyabe et al., 2023a), we can confirm that cybercrime encompasses a broad spectrum of activities, including computer hacking, identity theft, online fraud, malware attacks, denial-of-service (DoS) attacks, phishing, and malicious software distribution, all seeking economic gains, espionage, data theft, extortion, etc., being amongst the most prevalent. Our results reveal that cybercrime diversifies its attack methods, continuously growing in sophistication and diversity, making it challenging for companies to defend themselves (Fernández De Arroyabe and Fernández de Arroyabe, 2023; Jensen et al., 2021; Conteh and Schmick, 2016).

Moreover, our findings confirm existing literature (Fernandez de Arroyabe et al., 2023a), indicating that SMEs are potential targets of cybercrime. Similarly, our results show that no sector is immune to cyber incidents, ranging from opportunistic and indiscriminate attacks to sophisticated and highly selective campaigns against specific entities. In contrast to prior works that pointed to a sectorial bias towards IT technology sectors (Kabanda et al., 2018; Lezzi et al., 2018; Mirtsch et al., 2020; Nam, 2019), our results demonstrate that all sectors are susceptible to potential attacks due to the increasing prevalence of internet activities. Thus, we observe that the means employed by cybercriminals to execute cybercrime are rooted in the interconnected nature of businesses and the rising trend of internet activities within SMEs, thereby heightening their exposure to cyber incidents. Consequently, our results illustrate that cybercriminals exploit the vulnerabilities of SMEs to commit crimes that impact the SME, whether through financial gains, compromising data, or disrupting digital operations.

Concerning the analysis of Research Question 1 (RQ1), which revolves around the presence of fear and concern regarding cybercrime in SMEs, the findings related to fear and concern about potential

Table 16
Mean Values of Clusters.

VARIABLES	RANGE		CLUSTER 1	CLUSTER 2	CLUSTER 3	CLUSTER 4
	Minimum	Maximum	Mean	Mean	Mean	Mean
FEAR	0.00	24.00	15.889	9.8397	19.860	23.592
ACTIVITIES	.00	9.00	5.010	4.952	3.348	5.672
EXPERIENCE	.00	7.00	1.370	1.140	1.477	1.674
IMPACT	.00	9.00	1.688	1..095	1.663	2.193
TOTAL SMES			**5325**	**3638**	**785**	**1111**

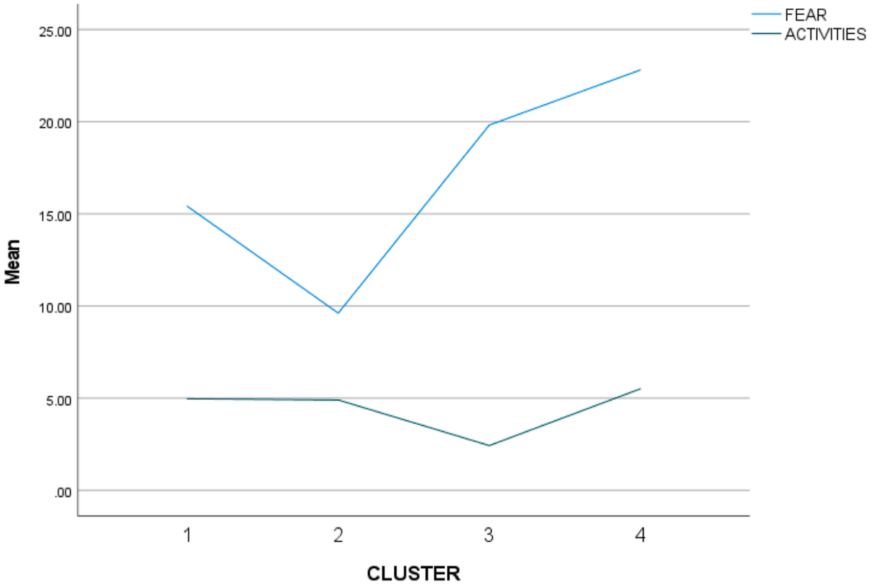


Fig. 1. Mean values of Fear and Activities by Cluster.

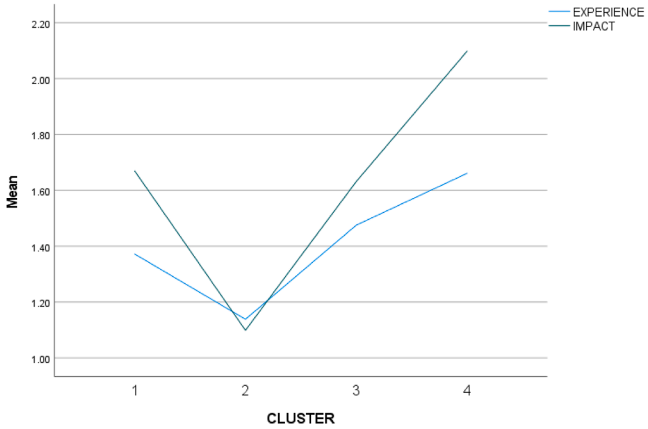


Fig. 2. Mean values of Experience and Impact by Cluster.

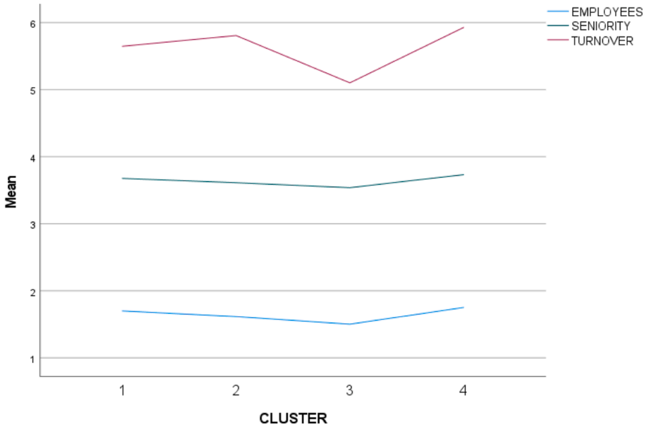


Fig. 3. Mean values of Employees, Seniority and Turnover.

cybercrime reveal a high degree of fear, shedding light on the ongoing debate surrounding the perception of cybercrime in terms of fear and concern (Fernandez de Arroyabe et al., 2023b). As we have indicated, our results indicate that SMEs are potential targets for cybercrime, thereby clarifying the stance of a certain body of literature that asserted SMEs believed they were not targets for cyberattacks. Our results are in line with previous works that demonstrate that the interconnected nature of business networks and the increased level of internet activities render all SMEs potential targets (Mirtsh et al., 2020; Nam, 2019). Additionally, we validate prior research by noting that certain SMEs restrain their online activities to mitigate exposure to networks and the potential dangers of cybercrime, resulting in a subsequent decline in economic activity (Fernandez de Arroyabe and Fernandez de Arroyabe, 2023).

Regarding RQ2, which investigates the factors influencing SMEs in experiencing fear and concern regarding cybercrime, our findings brighten key aspects of this intricate relationship. Firstly, our results affirm how internet activities impact the fear associated with cybercrime. The interconnectivity stemming from companies' internet activities exposes them to cybersecurity incidents arising from vulnerabilities in information technology usage, presenting security challenges (Arroyabe et al., 2024; Fernández de Arroyabe et al., 2023a,b; Benz and Chatterjee, 2020; Sule et al., 2021; Lezzi et al., 2018). Classic cyber threats such as spyware, malware, denial-of-service (DoS), ransomware,

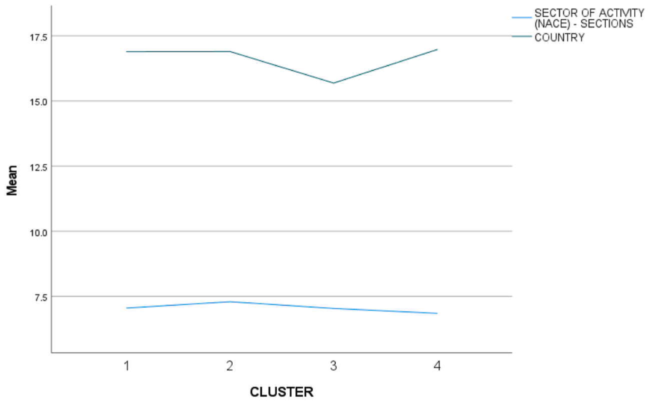


Fig. 4. Mean values of Sector and Countries by Cluster.

or phishing find potential entry points through interconnected devices in SMEs (Choo, 2011; Fernandez De Arroyabe and Fernandez de Arroyabe, 2023). The interconnected nature of digitization signifies that each inadequately protected device online potentially impacts the security and resilience of the enterprise (Corallo et al., 2020; Kabanda et al., 2018). Secondly, our results demonstrate that prior experiences influence fear towards cybercrime. Previous cyberattacks intensify the perception of cybercrime in SMEs, indicating that, on one hand, SMEs with limited cybersecurity resources may lack dedicated personnel or comprehensive measures, rendering them more susceptible. Fear of being ill-prepared to defend against sophisticated cyber threats becomes a source of concern. On the other hand, many SMEs heavily rely on digital operations for communication, transactions, and customer interactions. A successful cyberattack can disrupt these operations, instigating fear about potential impacts on daily business activities. Lastly, our findings substantiate that not only experiences but also being a target of attacks, with ensuing impacts on SMEs, should affect the perception of cybercrime. Cyberattacks can significantly impact the fear and concerns of SMEs for several reasons. Our results align with the literature indicating that the financial impact of a cyberattack, including costs related to remediation, potential legal actions, and loss of business, can be more severe for SMEs (ENISA, 2020). This financial strain can generate fear and anxiety about business sustainability. Furthermore, the fear of cybercrime can stem, from their reputation within local communities or market niches; a cyberattack causing data breaches or service interruptions can damage the trust that customers, partners, and stakeholders have in the SME. Therefore, fear of reputational harm can be a significant concern.

Continuing with Research Question 2 (RQ2), our results allow us to formulate a taxonomy on the perception of cybercrime in SMEs based on the explored clusters. The taxonomy provides a nuanced understanding of how different clusters of SMEs perceive and respond to cybercrime, considering factors such as fear, internet activities, impact, experience, and cybersecurity actions. Initially, we observed variability in the perception of fear related to cybercrime, and our findings enabled us to determine that this variability is derived from the internet activities conducted by SMEs, as well as their experiences and the impact of cybercrime. However, we note that fear is independent of SME characteristics such as size, sector, revenue, etc. Additionally, our observations indicate the significance of cybersecurity training in addressing the risks of cybercrime, along with the utilization of IT devices by workers. Below we show the taxonomy of the Perception of Cybercrime in SMEs by Clusters:

Cluster 1. *Balanced Engagement Cluster (*Moderate Fear, High Internet Activities, Moderate Impact and Experience*)*

Cluster 1 identifies a moderate level of fear regarding cybercrime, attributed to engagement in internet activities and encounters with cyber threats, particularly considering their impact. This finding aligns with existing literature, which notes that SMEs operating within the financial services sector tend to exhibit a moderate level of concern about cybercrime (Yeboah-Ofori et al., 2019; Saban et al., 2021). This concern is shaped by their level of involvement in online activities and their experiences with cyber threats, especially regarding the consequences of such incidents. According to Moneva and Leukfeldt (2023), SMEs in this sector adopt a balanced approach to their digital operations, engaging in internet activities to a high extent. Moreover, these SMEs experience a moderate level of impact from cybercrime and demonstrate an adequate level of proficiency in managing cybercrime incidents, corroborating previous works (Moneva and Leukfeldt, 2023). They also participate to a moderate degree in cybercrime training programs and advocate for the use of employee-owned devices in conducting online activities, indicating a comprehensive strategy toward cybersecurity practices.

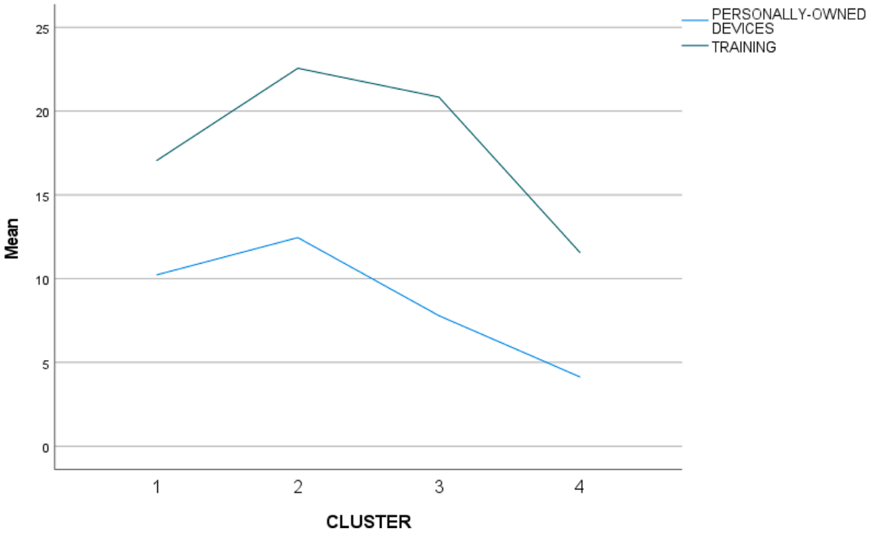
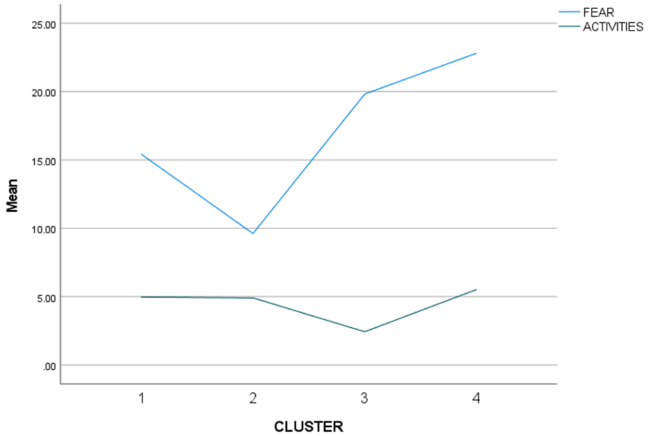
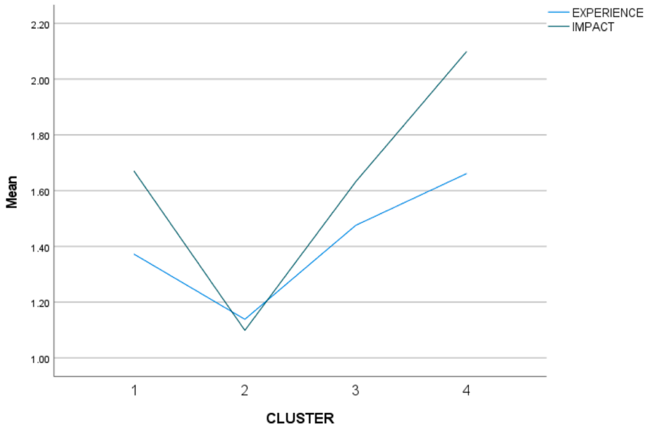


Fig. 5. Mean values of Personally-Owned Devices and Training by Cluster.



Cluster 2. *Proactive Telecommuting Cluster (*Lowest Fear, High Internet Activities, Lowest Impact and Experience*)*

Cluster 2 exhibits a notable pattern of high internet activity levels, yet records the lowest average values for fear, experiences, and impact compared to other clusters. This observation aligns with findings from previous studies, such as those by Yeboah-Ofori et al. (2019) and Saban et al. (2021), which highlight the paradoxical relationship between fear of cybercrime and engagement in online activities within SMEs, particularly in the manufacturing sector. Despite the low fear levels, this cluster demonstrates the highest involvement in training activities related to cybersecurity and the utilization of personal devices by employees. This trend suggests a prevalent culture of telecommuting within SMEs, wherein concerns about cybercrime risks may have been externalized (Ansong and Boateng, 2018). Moreover, the increased emphasis on cybersecurity training could potentially mitigate these concerns. In line with Caldeira and Ward (2002), within the manufacturing sector, SMEs show the lowest fear levels despite their active participation in high levels of internet activities. This indicates a nuanced perception of cybercrime risks, possibly influenced by organizational practices and training initiatives. Additionally, the manufacturing sector's high engagement in online activities underscores its dependence on digital operations.



Cluster 3. *Reactive Caution Cluster* (High Fear, Lowest Internet Activities, Moderate Impact and Experience)

Cluster 3 demonstrates the lowest level of engagement in internet activities compared to other clusters, suggesting that companies within this cluster, characterized by a heightened fear of cybercrime, adopt a reactive approach to the evolving landscape of online operations. Following Wong et al. (2022), this reactive attitude may be influenced by the elevated levels of experience with cybercrime, particularly the tangible damages incurred by SMEs. However, despite their reactive stance, these companies exhibit an active commitment to training activities aimed at mitigating the risks associated with cybercrime. For example, in the context of the retail sector, SMEs in this cluster display a high level of fear that responds to changes in online activities (Salam et al., 2021). This cautious approach is driven by the sector's experiences with cybercrime, particularly the tangible damages suffered. Notably, the SMEs within this cluster demonstrate the lowest level of engagement in internet activities, which, in line with Ibrahim et al. (2017), allows us to conclude that these SMEs reflect a reactive posture towards digital operations. Importantly, despite their lower involvement in internet activities, the sector remains actively engaged in training initiatives related to cybercrime risks, underscoring a steadfast commitment to cybersecurity practices. This finding corroborates previous research, which emphasizes the importance of proactive training efforts in enhancing SME cybersecurity (Moneva and Leukfeldt, 2023).

Cluster 4. *Impactful Resilience Cluster* (Highest Fear, Highest Internet Activities, Highest Impact and Experience)

Cluster 4 comprises companies exhibiting the highest levels of internet activities along with significant experience in dealing with cybercrime, particularly in terms of substantial damages incurred. As a result, these companies demonstrate the highest fear levels regarding cybercrime, yet they maintain an active approach toward the advancement of online operations. However, this proactive stance is not as pronounced in their engagement with cybercrime training activities or the utilization of IT devices by SME workers. For instance, within the Healthcare sector, which serves as an illustrative example, SMEs in this cluster exhibit the highest fear levels, influenced by their extensive internet activities and extensive experience with cybercrime, particularly concerning the significant damages incurred (Shah et al., 2019). Rachh (2021) points out that in the health sector, SMEs engage in the highest level of internet activities and demonstrate a proactive approach to digital operations. They possess the highest levels of impact and experience with cybercrime incidents, highlighting their comprehensive understanding of the associated challenges. However, despite their proactive attitude toward internet activities, the sector's engagement with cybercrime training and the utilization of IT devices by employees is comparatively less evident than in other sectors (Vuletić, 2017). This finding is consistent with prior research by Moneva and Leukfeldt (2023), which underscores the importance of a holistic approach to cybersecurity readiness, encompassing both proactive measures and employee training initiatives.

6. Conclusion

In conclusion, this study has applied Cyberspace Theory to analyse cybercrime in SMEs, providing a comprehensive characterization of cyber criminals and their activities. Unlike previous research focusing solely on cyberattacks or cybersecurity measures, Cyberspace Theory has allowed us to delve into the motives, objectives, routines, and vulnerabilities contributing to cyber threats. Our findings confirm the diverse methods employed by cybercriminals, including computer hacking, identity theft, online fraud, malware attacks, denial-of-service (DoS) attacks, phishing, and malicious software distribution. Cybercrime continues to evolve in sophistication and diversity, posing challenges for SMEs to defend themselves.

Furthermore, our results reaffirm that SMEs are potential targets for cybercrime across various sectors. Contrary to the notion that only larger companies face significant cyber threats, our study demonstrates that all sectors, due to increased internet activities, are susceptible to cyber incidents. The interconnected nature of businesses and the growing trend of internet usage heighten SMEs' exposure to cyber threats, as cybercriminals exploit vulnerabilities for financial gains, data compromise, and disruptions to digital operations.

Analysing research questions, our findings indicate a high degree of fear amongst SMEs, challenging previous beliefs that SMEs are not prime targets. The interconnected nature of business networks and heightened internet activities render all SMEs potential targets, impacting economic activity. Moreover, we reveal that internet activities and prior experiences significantly influence fear and concern about cybercrime. Cybersecurity incidents arising from internet activities expose SMEs to threats, while prior cyber attacks intensify fear. Being a target of attacks further impacts SMEs' perception of cybercrime, with financial implications and concerns about reputation within communities or market niches.

The formulated taxonomy based on explored clusters provides a nuanced understanding of how SMEs perceive and respond to cybercrime. The variability in fear is linked to internet activities, experiences, and the impact of cybercrime, independent of SME characteristics. The taxonomy highlights the significance of cybersecurity training and IT device utilization in addressing cyber threats. Overall, this study contributes valuable insights for SMEs to enhance their cybersecurity strategies and adapt to the evolving landscape of cyber threats.

A *theoretical contribution* to Cyberspace Theory in the realm of cybercrime within SMEs involves integrating dynamic elements into this framework. Thus, there is a necessity to introduce a temporal dimension to cybercrime, recognizing the evolving nature of cyber threats over time, including the cyclical tactics employed by cybercriminals and the adaptive behaviours of both offenders and potential victims. The extended theory introduces the concept of a suitable target, expanding its scope to encompass various components of cyberspace. This acknowledges that not only the organization itself but also its digital assets, online presence, and interconnected networks are pivotal factors. The absence of capable guardians is not limited to physical presence; it also encompasses effective cybersecurity measures, incident response capabilities, and collaborative efforts within the cyber ecosystem. Additionally, considering the asymmetry of information in cyberspace becomes crucial, recognizing that potential offenders may possess a higher level of technical expertise, leaving SMEs lacking awareness and understanding of evolving cyber threats. This information gap significantly influences routine activities, rendering SMEs more susceptible to cybercrime. Furthermore, the enhanced Cyberspace framework incorporates the adaptability of cybercriminals, distinguishing them from traditional criminals. Cyber offenders continually adjust their methods, presenting challenges for SMEs in predicting and defending against potential threats. The routine activities of cybercriminals involve exploiting emerging vulnerabilities, staying informed about security measures, and adapting to countermeasures. Finally, the Cyberspace framework introduces the concept of a cybersecurity culture within organizations, evaluating how the routine activities of employees, their awareness of cybersecurity practices, and the organizational emphasis on security collectively contribute to overall resilience against cyber threats. A robust cybersecurity culture serves as a proactive guardian against potential cybercrime. By incorporating these dynamic elements, Cyberspace Theory evolves into a more comprehensive framework for comprehending cybercrime in SMEs. This adaptation addresses the distinctive challenges posed by the rapidly changing nature of cyber threats and the intricate interplay of factors within the digital environment.

As second contribution, we have developed *managerial implications*. SMEs must adopt and consistently update robust cybersecurity measures to counter the dynamic nature of cyber threats. This involves investing in advanced technologies, providing regular employee training, and fostering a cybersecurity culture within the organization. Additionally, recognizing the influence of prior experiences on fear and concern, SMEs should institute tailored training programs to augment the cybersecurity awareness and skills of employees. These programs should encompass not only basic security practices but also address specific threats and vulnerabilities relevant to the organization. Conducting dynamic risk assessments is crucial for SMEs to adapt to the evolving cyber threat landscape. This process entails regularly evaluating the organization's online activities, potential vulnerabilities, and the efficacy of existing cybersecurity measures. Furthermore, engaging in collaborative efforts is essential. Given the interconnected nature of the digital environment, SMEs should actively participate in collaborative initiatives within the cyber ecosystem. This involves sharing threat intelligence, adopting best practices, and collaborating with industry peers to enhance overall cybersecurity resilience. Lastly, having a proactive incident response is a key factor. SMEs must develop and consistently update incident response plans to efficiently address and mitigate the impact of cyber incidents, thereby minimizing financial losses and reputational damage.

Lastly, we have included *political implications*. Policymakers play a pivotal role in addressing cybercrime challenges faced by SMEs. Recognizing the susceptibility of SMEs to cyber threats, policymakers should formulate supportive policies. This may involve offering financial incentives for cybersecurity investments, developing training programs, or establishing regulatory frameworks that foster a cybersecurity culture. Governments can further contribute by creating information-sharing platforms for SMEs to exchange insights on cyber threats and incidents. Facilitating collaboration amongst SMEs, larger enterprises, and governmental agencies enhances the overall cybersecurity resilience. Policymakers should also focus on developing clear and attainable regulatory frameworks concerning cybersecurity for SMEs. Compliance with these regulations encourages the implementation of necessary cybersecurity measures and cultivates a culture of cyber resilience. Initiating public awareness campaigns is another avenue for governments to educate SMEs about prevalent cyber threats and emphasize the significance of cybersecurity, fostering proactive cybersecurity practices. Policymakers should invest in capacity-building initiatives for SMEs, providing resources and support for the development of cybersecurity capabilities. This includes training programs, access to cybersecurity experts, and financial assistance for adopting advanced technologies. In summary, the collaboration between managers and policymakers is paramount in effectively addressing cybercrime challenges in SMEs. While managers focus on cybersecurity measures, employee training, and collaboration, policymakers play a vital role in creating a supportive regulatory environment, facilitating information sharing, and building SME capacity to combat cyber threats effectively.

While our study contributes valuable insights into the perception of cybercrime in SMEs, it is essential to acknowledge certain limitations. Firstly, the generalizability of our findings may be constrained due to the specific context and sample characteristics. The study focuses on SMEs within a certain geographic area and industry sectors, and variations across different regions or sectors may exist. Additionally, the use of a cross-sectional design limits our ability to establish causal relationships or capture changes over time. Longitudinal studies would provide a more comprehensive understanding of the dynamics involved. Furthermore, the reliance on self-reported data introduces the possibility of response bias, as participants might underreport or over report certain aspects. Future research could employ a mixed-methods approach or incorporate objective measures to enhance data validity. Lastly, our study primarily emphasizes the quantitative aspect, and a qualitative exploration could offer a deeper understanding of the nuances surrounding SMEs' experiences and perceptions of cybercrime. These limitations, while inherent to the study design, highlight areas for potential refinement and further investigation in future research endeavours.

CRediT authorship contribution statement

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

Data curation, Conceptualization.

Declaration of competing interest

The authors state that they have no conflict of interest in the paper.

Data availability

The authors do not have permission to share data.

References

Adams, J., Albakajai, M., 2016. Cyberspace: a new threat to the sovereignty of the state. J. Manag. Stud. 4 (6), 256–265.

Albakjaji, M., Adams, J., Almahmoud, H., Al Shishany, A.S., 2020. The legal dilemma in governing the privacy right of e-commerce users: evidence from the USA context. Int. J. Serv. Sci. Manag. Eng. Technol. 11 (4), 166–187.

Ansong, E., Boateng, R., 2018. Organisational adoption of telecommuting: evidence from a developing country. Electron. J. Inf. Syst. Dev. Countries 84 (1), e12008.

Arroyabe, M.F., Arranz, C.F.A., Arroyabe, I.F.D., Fernandez De Arroyabe Fernandez, J.C, 2024. The effect of IT security issues on the implementation of industry 4.0 in SMEs: barriers and challenges. Technol. Forecast. Soc. Change 199, 123051. -123051.

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

Bella, D., Katsinis, L., Lagüera-González, A., Odenthal, J., Hell, L., Lozar, M., 2023. Annual Report on European SMEs 2022/2023. SME Performance Review 2022/2023. European Commission. https://single-market-economy.ec.europa.eu/system/files/2023-08/Annual%20Report%20on%20European%20SMEs%202023_FINAL.pdf.

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

Bertino, E., Choo, K.K.R., Georgakopolous, D., Nepal, S., 2016. Internet of Things (IoT) smart and secure service delivery. ACM Trans. Internet Technol. 16 (4), 22–29.

Boswell, R., 2023. 60% of European SMEs That are Cyber-Attacked Have to Close After Six Months. Startup Magazine. https://startupsmagazine.co.uk/article-60-european-smes-are-cyber-attacked-have-close-after-six-months.

Brands, J., van Wilsem, J., 2021. Connected and fearful? Exploring fear of online financial crime, internet behaviour and their relationship. Eur. J. Criminol. 18, 213–234.

Brenner, S.W., 2010. Cybercrime: Criminal Threats from Cyberspace. Bloomsbury Publishing USA.

Caldeira, M.M., Ward, J.M., 2002. Understanding the successful adoption and use of IS/IT in SMEs: an explanation from Portuguese manufacturing industries. Inf. Syst. J. 12 (2), 121–152.

Caton, J.F., 2012. On the Theory of Cyberspace. Strategic Studies Institute, US Army War College. https://www.jstor.org/stable/pdf/resrep12116.26.pdf.

Chief Healthcare Executive (2024). More than 88 million people have been affected by health data breaches this year. https://www.chiefhealthcareexecutive.com/view/more-than-88-million-people-have-been-affected-by-health-data-breaches-this-year.

Choi, J., Kruis, N.E., Choo, K.S., 2021. Explaining fear of identity theft victimization using a routine activity approach. J. Contemp. Crim. Justice 37, 406–426.

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

CISA,gov, 2020. Cyberspace Policy Review, 2009. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/resources-tools/resources/2009-cyberspace-policy-review.

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

Cook, S., Giommoni, L., Trajtenberg Pareja, N., Levi, M., Williams, M.L., 2023. Fear of economic cybercrime across Europe: a multilevel application of Routine Activity Theory. Br. J. Criminol. 63 (2), 384–406.

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

Dąbrowska, J., Almpanopoulou, A., Brem, A., Chesbrough, H., Cucino, V., Di Minin, A., Ritala, P., 2022. Digital transformation, for better or worse: a critical multi-level research agenda. R&D Manag. 52 (5), 930–954.

Dalenogare, L.S., Benitez, G.B., Ayala, N.F., Frank, A.G., 2018. The expected contribution of Industry 4.0 technologies for industrial performance. Int. J. Prod. Econ. 204, 383–394.

Deloitte, 2020. 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.

Dudek, A., 2020. Silhouette index as clustering evaluation tool. In: Classification and Data Analysis: Theory and Applications, 28. Springer International Publishing, pp. 19–33.

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

European Union, 2022. Eurostat, Flash Eurobarometer No. 496. Eurobarometer. European Commission. https://europa.eu/eurobarometer/surveys/detail/2280.

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

Fernandez De Arroyabe, I., Fernandez de Arroyabe, J.C., 2023. The severity and effects of Cyber-breaches in SMEs: a machine learning approach. Enterpr. Inf. Syst. 17 (3), 1942997.

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

Fox, J., 2024. Top Cybersecurity Statistics for 2024. Cobalt. https://www.cobalt.io/blog/cybersecurity-statistics-2024#:~:text=75%25%20of%20security%20professionals%20have,burden%20on%20organizations%20.

Fraley, C., Raftery, A.E., 2002. Model-based clustering, discriminant analysis, and density estimation. Am. Stat. Assoc. 97 (458), 611–631.

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

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

Ibrahim, N.F., Wang, X., Bourne, H., 2017. Exploring the effect of user engagement in online brand communities: evidence from Twitter. Comput. Human Behav. 72, 321–338.

Jensen, M.L., Durcikova, A., Wright, R.T., 2021. Using susceptibility claims to motivate behaviour change in IT security. Eur. J. Inf. Syst. 30 (1), 27–45.

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

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

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

Mamat, A.R., Mohamed, F.S., Mohamed, M.A., Rawi, N.M., Awang, M.I., 2018. Silhouette index for determining optimal k-means clustering on images in different color models. Int. J. Eng. Technol. 7 (2), 105–109.

Manesh, M.F., Pellegrini, M.M., Marzi, G., Dabic, M., 2020. Knowledge management in the fourth industrial revolution: mapping the literature and scoping future avenues. IEEE Trans. Eng. Manage. 68 (1), 289–300.

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

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

Moeuf, A., Lamouri, S., Pellerin, R., Tamayo-Giraldo, S., Tobon-Valencia, E., Eburdy, R., 2019. Identification of critical success factors, risks and opportunities of industry 4.0 in SMEs. Int. J. Prod. Res. 58 (5), 1–17.

Moneva, A., Leukfeldt, R., 2023. Insider threats among Dutch SMEs: nature and extent of incidents, and cyber security measures. J. Criminol. 56 (4), 416–440.

Moody, R., 2024. Since 2018, Ransomware Attacks on the Education Sector Have Cost the World Economy Over $53 Billion in Downtime Alone. Comparitech. https://www.comparitech.com/blog/vpn-privacy/school-ransomware-attacks-worldwide/.

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

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

Papakonstantinou, V., 2010. Cyberspace and cybercrime. Handbook of Electronic Security and Digital Forensics, pp. 455–476.

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

Poireault, K. (2024). Manufacturing top targeted industry in record-breaking cyber extortion surge. https://www.infosecurity-magazine.com/news/manufacturing-top-targeted-orange/.

Rachh, A., 2021. A study of future opportunities and challenges in digital healthcare sector: cyber security vs. crimes in digital healthcare sector. Asia Pacific J. Health Manag. 16 (3), 7–15.

Rahmonbek, R., 2024. 35 Alarming Small Business Cybersecurity Statistics for 2024. StrongDM. https://www.strongdm.com/blog/small-business-cyber-security-statistics.

Saban, K.A., Rau, S., Wood, C.A., 2021. SME executives' perceptions and the information security preparedness model. Information & Computer Security 29 (2), 263–282.

Salam, M.T., Imtiaz, H., Burhan, M., 2021. The perceptions of SME retailers towards the usage of social media marketing amid COVID-19 crisis. J. Entrepreneurship Emerg. Econ. 13 (4), 588–605.

Shah, M.H., Jones, P., Choudrie, J., 2019. Cybercrimes prevention: promising organisational practices. Inf. Technol. People 32 (5), 1125–1129.

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

Vial, G., 2021. Understanding Digital Transformation: A Review and a Research Agenda. Managing digital Transformation. Routledge.

Vuletić, I., 2017. Data-driven healthcare and cybercrime: a threat we are not aware of. Asia Pacif. J. Health Law Ethics 11 (2), 16–32.

Walden, I., 2005. Crime and security in cyberspace. Cambridge Rev. Int. Affair. 18 (1), 51–68.

Wall, D.S., 2007. Policing cybercrimes: situating the public police in networks of security within cyberspace. Police. Pract. Res. 8 (2), 183–205.

Wong, L.W., Lee, V.H., Tan, G.W., Ooi, K.B., Sohal, A., 2022. The role of cybersecurity and policy awareness in shifting employee compliance attitudes: building supply chain capabilities. Int. J. Inf. Manage. 66, 102520.

World Bank Finance, 2021. Improving SMEs' Access to Finance and Finding Innovative Solutions to Unlock Sources of Capital. https://tinyurl.com/2ap98wrn.

Yeboah-Ofori, A., Abdulai, J., Katsriku, F., 2019. Cybercrime and risks for cyber-physical systems. Int. J. Cyber-Secur. Digit. Forensic. 8 (1), 43–57.

Marta F. Arroyabe is a Reader and Deputy Head of the Strategy Operations and Entrepreneurship (SOE) Group at Essex Business School. Marta's research focuses on four primary areas: innovation, digitalisation & cybersecurity, environmental management, and entrepreneurship. In the area of innovation, her research aims to understand the development and implementation of innovation in firms and explores firms' innovation decisions and strategies. In digitalisation and cybersecurity, her research investigates the intersection of IT security, digital transformation, and cybersecurity resilience in SMEs. Her research investigates the digitalisation dynamics in SMEs, emphasising the multifaceted nature of drivers, interactions, and the overall decision-making process within the evolving landscape of Industry 4.0. Her research also delves into the strategic decision-making behind cybersecurity investments in SMEs and provides an understanding of how cybersecurity challenges, capabilities and organisations' external environment intersect with the broader landscape of digital transformation and strategic decision-making within SMEs, aiming to shed light on practical aspects that can enhance resilience and decision-making in the face of evolving cyber threats. In the area of environmental management, she primarily focuses on two topics, eco-innovation and circular economy, where she studies business responses to improving environmental performance and to increasing societal concerns for the environment. Her research explores the development of eco-innovation and circular economy business models in firms and the impact of these on firms' performance. Finally, in the area of entrepreneurship, her research primarily focuses on entrepreneurial education and entrepreneurial intention. Her work aims to understand to which extent entrepreneurial education in higher education institutions (such as universities) spurs students' entrepreneurial intention and fosters entrepreneurial activity. She has published her work in *"Journal of Business Research", "R&D Management", "Technovation", "Studies in Higher Education", "British Journal of Management", "European Journal of Innovation Management", "Technology Analysis and Strategic Management", "Journal of Cleaner Production", "Technological Forecasting and Social Change", "Journal of Computer Information Systems" or "Computers and Security".*

Carlos F.A. Arranz is a Lecturer in Business Operations at the University of Greenwich. His-main research interest centres on the application of Machine Learning methods to the analysis of business, particularly on the implementation of Circular Economy Models. He holds a PhD in Business Analytics from Essex Business School (University of Essex), an MRes in International Political Economy from the London School of Economics and Political Science (LSE), and an MRes in Economics and Finance from the Université du Luxembourg. Before that, he received a BSc in Economics and Business Economics (International Economics Studies Specialisation) from Maastricht University.

Ignacio Fernandez de Arroyabe is Cyber Risk Manager in Lloyds Bank Commercial Banking (UK). He has worked in cybersecurity in Jaguar Land Rover in the UK. His-research interests are in cybersecurity risk management in the firms. He is a PhD candidate in cybersecurity at Loughborough University.

Juan Carlos. Fernandez de Arroyabe is a Professor in Essex Business School (University of Essex). His-research interests include joint R&D projects, R&D networks, cybersecurity, and complex technological systems. He is author or co-author of numerous papers published in the *British Journal of Management, Computer and Security; IEEE Transaction Engineering Management, the Complexity, Technovation, Studies in Higher Education, Journal Cleaner Production, Business Strategy and The Environment, Journal Business Research; Emergence: Organization and Complexity, Technological Forecasting Social Change, Journal of Enterprise Information Management, International Small Business Journal, European Journal of Work and Organisational Psychology, Scandinavian Journal of Tourism, and Industry Higher Education.* Also, he is Associate Editor of the Journal of Entrepreneurship in Emerging Economies and member of Editorial Board of Technological Forecasting Social Change.