María Isabella Mora Napolitano

The Impact of Cybercrime on the enterprises: A Comparison Between SMEs and Larger Corporations in Catalonia

Final Degree Thesis

Thematic Area: Business & Society

Business Administration and Management

FACULTAT D'ECONOMIA i EMPRESA
Universitat Rovira i Virgili

Reus

2024-25

Table Of Contents

List of Tables

List of Figures

Abstract

Títol: L'Impacte del Cibercrim a les Empreses: Una Comparativa entre PIMEs i Grans Corporacions a Catalunya

Aquest estudi analitza com les petites i mitjanes empreses (PIMEs) i les grans corporacions a Catalunya afronten els ciberatacs, amb l'objectiu d'identificar diferències en estratègies, vulnerabilitats i impactes des d'una perspectiva d'Administració d'Empreses. Mitjançant una revisió bibliogràfica de 25 estudis i entrevistes semiestructurades a vuit empreses i cuatre professionals del sector, la investigació confirma quatre hipòtesis basades en teories com la Visió Basada en Recursos (VBR), la Teoria de la Cultura Organitzativa i el Model d'Acceptació Tecnològica (TAM).

Els resultats revelen que les grans empreses exhibeixen una major consciència i estratègies estructurades (com protocols proactius i formació contínua), mentre que les PIMEs adopten enfocaments reactius, amb dependència d'externs i limitacions de recursos. Les PIMEs pateixen impactes més greus davant ciber incidents, mentre que les corporacions redueixen danys gràcies a plans de resposta ràpida.

Des d'una perspectiva sociològica, la cultura organitzativa i les normes de comportament influeixen en la preparació davant amenaces, amb una major transparència en grans empreses durant crisis. Les implicacions pràctiques subratllen la necessitat d'integrar la ciberseguretat com a element estratègic: les PIMEs poden millorar mitjançant formació bàsica i col·laboració externa, mentre que les grans corporacions han d'actualitzar-se contínuament i fomentar una cultura de seguretat interna. Aquesta recerca aporta un marc per entendre com la mida empresarial modela la resiliència digital, combinant rigor tècnic amb dinàmiques humanes i organitzatives.

Paraules clau: Ciberseguretat, gestió del risc, cultura organitzativa.

Título: El Impacto del Cibercrimen en las Empresas: Una Comparativa entre PYMES y Grandes Corporaciones en Cataluña

Este estudio explora cómo las pequeñas y medianas empresas (PYMES) y las grandes corporaciones en Cataluña enfrentan los ciberataques, con el objetivo de identificar diferencias en estrategias, vulnerabilidades e impactos desde una perspectiva de Administración de Empresas. Mediante una revisión bibliográfica de

25 estudios y entrevistas semiestructuradas a ocho empresas y cuatro profesionales del sector, la investigación confirma cuatro hipótesis basadas en teorías como la Visión Basada en Recursos (VBR), la Teoría de la Cultura Organizativa y el Modelo de Aceptación Tecnológica (TAM).

Los resultados revelan que las grandes empresas muestran mayor conciencia y estrategias estructuradas (como protocolos proactivos y formación continua), mientras que las PYMES adoptan enfoques reactivos, con dependencia de proveedores externos y limitaciones de recursos. Las PYMES sufren impactos más graves ante ciber incidentes, mientras que las corporaciones mitigan daños gracias a planes de respuesta rápida.

Desde una perspectiva sociológica, la cultura organizativa y las normas de comportamiento influyen en la preparación ante amenazas, con mayor transparencia en grandes empresas durante las crisis. Las implicaciones prácticas destacan la necesidad de integrar la ciberseguridad como elemento estratégico: las PYMES pueden mejorar mediante formación básica y colaboración externa, mientras que las grandes corporaciones deben actualizarse continuamente y fomentar una cultura de seguridad interna. Esta investigación aporta un marco para entender cómo el tamaño empresarial moldea la resiliencia digital, combinando rigor técnico con dinámicas humanas y organizativas.

Palabras clave: Ciberseguridad, gestión del riesgo, cultura organizativa.

Title: The Impact of Cybercrime on Enterprises: A Comparison Between SMEs and Larger Corporations in Catalonia

This study examines how small and medium-sized enterprises (SMEs) and large corporations in Catalonia address cyberattacks, aiming to identify differences in strategies, vulnerabilities, and impacts from a Business Management perspective. Through a literature review of 25 studies and semi-structured interviews with eight companies and four cybersecurity professionals, the research confirms four hypotheses grounded in theories such as the Resource-Based View (RBV), Organizational Culture Theory, and Technology Acceptance Model (TAM).

Findings reveal that large corporations exhibit higher awareness and structured strategies (e.g., proactive protocols and continuous training), while SMEs rely on reactive approaches, external providers, and face resource constraints. SMEs suffer

more severe impacts from cyber incidents, whereas large firms mitigate damages through rapid response plans.

From a sociological perspective, organizational culture and behavioral norms shape threat preparedness, with large firms demonstrating greater transparency during crises. Practical implications emphasize integrating cybersecurity as a strategic element: SMEs can improve through basic training and external collaboration, while large corporations must prioritize continuous adaptation and foster an internal security culture. This research provides a framework to understand how company size shapes digital resilience, bridging technical rigor with human and organizational dynamics.

Keywords: Cybersecurity, risk management, organizational culture.

Presentation

Choosing the topic of cybersecurity in businesses was the result of several combined factors, including both my personal and academic experiences. The most influential factor that led me to focus on this topic was my experience writing a thesis abroad. That thesis explored how different economic factors affected theft in a society. Thanks to this economic perspective on crime, I became more aware of the importance of exploring similar issues more deeply, but from a more social and modern point of view, this is why I chose cybercrime.

In addition, this topic is very current and relevant in our society. We live in a digital world, where we increasingly see more sophisticated cyberattacks that adapt to our technological abilities. These threats affect all individuals and begin to spread through societies, regardless of their size. Everyone should understand these changes and learn to protect essential elements such as data, financial assets, and overall operational integrity.

What interested me was the contrast between how small and medium-sized enterprises (SMEs) and large corporations deal with these threats, considering their differences in resources, perception of risk, and security strategies.

The skills I developed during my degree, such as critical thinking, analytical reasoning, and a solid understanding of financial and management principles, are directly connected to this research. They helped me analyze the technical side of cybersecurity and its strategic impact on reputation, business continuity, and risk management.

More specifically, through different subjects in my bachelor's degree, I gained a variety of perspectives. For example, in Business Research Methods, I learned how to collect data through literature analysis and semi-structured interviews, and how to apply analytical thinking to interpret this information. In Knowledge Development in International Firms, we covered how global businesses adapt to fast-changing trends and the importance of organizational culture. This was further supported by the course Human Resource Management, where we focused on topics such as ethics and corporate social responsibility.

By exploring this topic, I hope to contribute to the ongoing conversation about cybersecurity in the business world, emphasizing the role of strategic decisions,

human factors, and the growing need for proactive cybersecurity policies. My goal for this research is to offer useful insights to both SMEs and large companies in developing stronger cybersecurity strategies and to study the importance of organizational culture within a company and how it affects decisions regarding cybersecurity procedures.

Chapter 1: Introduction

Today's World is characterized by its flexibility and forced fast adaptation to technology. Topics such as cybersecurity and cybercrime have risen in importance because companies and individuals feel pressure towards these changes (Manky, 2013:9).

A December 2018 study from Cambridge pointed out that 55 percent of enterprises showed at least one data breach in a one-year gap (Zielinski, 2019). This is clear evidence that these topics are undoubtedly a daily routine for all enterprises.

Concepts such as cybercriminals have been brought up in each study of cybersecurity. These characters show a clear evolution throughout the years in their tactics, presenting an image of sophisticated scammers (Amrin, 2014: 9). This explains how quickly these characters adapt to the new advancements and periods of technology. Additionally, the new incorporation of the now well-known tool Artificial Intelligence (AI) creates a significant positive opportunity for how the World is perceived, but also motivates cybercriminals to find ways to exploit digital payments (Singer & Pratt, 2016). Recent cases involving AI through voice imitation have been more frequent and not only highlight the possible vulnerabilities of today's enterprises and give space to analyze and focus on investigating the response and consequences such acts have on businesses (Santos, 2024).

More particularly concerning is the situation of small and medium enterprises (SMEs), which are characterized (from a cybersecurity point of view) as being more susceptible to such crimes because they lack the resources and technical expertise needed to implement and, more importantly, prevent frauds via digital media forms (Vijayakumar and Ilangovan, 2015:90).

On the other hand, large enterprises work as their obvious counterparts since they typically have dedicated teams and budgets for managing cyber risks. However, this does not mean that these types of companies are excluded from these risks because although they do have a specific fund to prevent and control cyberattacks they are facing more complex challenges due to their size; in other words; greater visibility and reliance on the legal system (Epstein, 2023: 33).

In other words, cybercrime has become a crucial concern for businesses, no matter their size. Other studies done in this field of work conclude that not only is the

financial impact an important matter, but also the reputational image left by what that company gives to the public and, more specifically, to their clients (PwC, 2020:7).

This research aims to analyze how SMEs and large enterprises in Catalonia are addressing the growing challenge of cybercrime in today's society of frequent digital transformation. From the Business Administration and Management perspective, understanding this kind of area and how to manage these risks from different spaces within a company is important since its effectiveness is linked not only as a technical internal issue but also involves strategic decision-making.

SMEs are defined (as Spanish law presents) as any company whose structure consists of fewer than 250 employees, has less than 50 million EUR in annual turnover, and constitutes part of the private sector (Ley 14/2013, de 27 de septiembre, de Apoyo a los emprendedores y su internacionalización, 2013).

On the contrary, larger companies are defined as enterprises that pass the thresholds for SMEs, typically having more than 250 employees and annual revenue greater than 50 million EUR (European Commission Recommendation 2003/361/EC, 2003).

This was done through the analysis of 25 case studies that show evidence justifying or denying the real risks of these types of attacks for both SMEs and large enterprises. I selected these articles primarily due to their established credibility, as demonstrated by their consistent citation in the academic community. Additionally, I prioritized studies that contributed valuable findings, ensuring their relevance to the research at hand.

One of the studies used as the main base for this research was Alahmari and Duncan's study (2020), in which they conducted a systematic literature review using software called NVivo to explore cybersecurity risk management in SMEs.

Therefore, this study follows the three-stage methodology mentioned in Alahmari and Duncan's (2020) study. These stages consist of planning the review by defining the scope and developing a protocol. Then, we can conduct the review by identifying, selecting, and analyzing relevant studies, and last but not least, reporting findings and making recommendations (Alhamari & Duncan, 2020:3). Nevertheless, this study does not focus on doing a systematic review due to the complexity of this process and the limitations of resources.

The review utilized databases such as Scopus, IEEE, and SpringerLink to search for articles published between 2015 and 2024. Only empirical studies focusing on this topic were included, so a "round of dismissal" was implemented. The analysis involved a profound analysis using different AI software with human participation to extract themes and patterns, similar to Alahmari and Duncan's method, which identified five key perspectives: threats, behaviors, practices, awareness, and decision-making. The analysis helps create a more adequate image of the different perceptions of this type of fraud and was used as a starting point to frame the literature review and ensure that the focus of this thesis work remains aligned with the defined objectives.

Additionally, multiple local companies (eight) were interviewed (four SMEs and four larger companies) so a more specific and real point of view could be extracted to understand and compare the damages and opportunities each has. This provides a practical view on this case since the responses extracted from the interviews will bring many points of reference because this issue depends on the area of work within the company. Simply put, the answers are expected to vary depending on the interviewee's expertise[1].

These companies were deliberately selected to gain multiple perspectives on the similarities and differences between their size and sector. By using a comparative method between SMEs and larger companies, this study seeks to reveal each size's advantages and disadvantages and uncover unthought commonalities between the two. This approach recognizes that cybersecurity is a multidimensional issue.

In addition, four professionals working in the field were successfully contacted to provide deeper expertise on the topic. Their perspectives were essential for this thesis, as they offered first-hand insights based on their active experience in the cybersecurity sector in Catalonia.

The companies' representatives and cybersecurity professionals (the interviewees) were asked for their opinions on the disclosure of the data and their privacy. The individuals were treated as anonymous, and therefore, their answers will be extracted using a pseudonym, thereby respecting the ethical standards of academic research.

[1] It will not be the same questioning someone from the human resources department as with someone from the IT department.

The interviews were conducted face-to-face, with the exception of one interview, which was conducted online due to the impossibility of finding a mutually convenient schedule. Each time, the same questions were asked to provide a standardized process and recollection of the data. The query was in an open-answer format so the person being inquired could provide a more reasonable and justified answer and also a more in-depth response.

The structure of this research paper consists mainly of two blocks. In the first section, key concepts and the context of the main ideas and past studies are introduced, and the second section consists of the analysis and research of the value added.

By examining the impact of cybercrime on Catalonian enterprises, this thesis seeks to contribute to the growing body of knowledge in this search field and provide insights that can inform and help not only Catalonian companies (although it is focused on this space) but also the overall sectors of SMEs and larger companies understand the magnitude of importance cybersecurity has nowadays.

This work is beneficial and consequential for future approaches and development in the fields of business and management, cybersecurity and cybercrime, enterprise policies, and digital forms of fraud, among others. It can be used as a guide for further advancements in these interlocked fields. It can also help past studies since, as many authors proclaim, the study has an existing gap (Chidukwani, Zander & Koutsakis, 2022:12).

Additionally, this topic is considered mainstream interest because of its fast-growing nature and how its repercussions influence the routine of doing and viewing things.

For this methodology, it was crucial to establish objectives, and they are as follows:

General objectives: Analyze how SMEs and larger enterprises in Catalonia react to the ongoing and emerging cybercrime challenges from a Business and Management perspective, exploring their strategies, vulnerabilities, and opportunities, also known as a SWOT analysis.

Specific objectives: Identify the more frequent risks linked to cybercrime in SMEs and larger companies; determine the differences in resources and actions between the two when a cyber threat is presented; value the reputational value this leads to

depending on the size and sector; and propose recommendations and future approaches for scholars, people interested in this topic, and companies themselves to strengthen cybersecurity.

In summary, this thesis aims to analyze how SMEs and large enterprises in Catalonia address the growing challenge of cybercrime from a Business Administration and Management perspective. Its goal is to question the differences in strategies and perceptions between organizations of assorted sizes and sectors, and the role of human resources and organizational culture in providing this risk. The outcome is expected to shed light on the gaps in this field of study and strengthen the existing work. The methodology involves a literature review and interviews with representatives from SMEs and large enterprises to gain a practical, real-world understanding of the challenges and strategies employed.

Chapter 2: Thesis Development

Considering the estimated time for each phase and its final deadline, the following timeline has been established:

Table 1. Schedule of Main Activities for this Degree Thesis.

STAGE	**MAIN ACTIVITY/ACTION**	**NOTES TO CONSIDER**	**MONTHS**
STAGE I: Preparation	Structure design, literature, and company selection.	Periodic meetings.	December.
STAGE II: Data Collection	Review of articles/news + interviews.	Meetings focused on the	January - February.

		more practical aspects.	
STAGE III: Analysis of Findings	Written interpretation linked to the literature. Initial comparison.	Continuous reading and review.	March.
STAGE IV: Results Writing	Results and conclusion.	Deepen understanding.	April.
STAGE V: Final Closure	Conclusions, final editing, and submission.	Final review. Explanatory video (presentation). Guided practice.	May - June.

Source: Author's own elaboration.

As can be seen, it was decided to focus and divide the work into strategic phases of the methodology, totaling five phases. It is important to note that this is an ideal schedule but not inflexible, so the stages are separated by months rather than by a day count.

The first phase is where the topic is already focused, and the goals define the structure and objectives of the thesis. In this phase, the maximum amount of literature is collected, eliminating what does not align with the objectives. Additionally, this phase involves selecting the eight companies that will provide data for the more practical part of the work.

Thus, the key activities are summarized in the review of the topic, the definition of objectives, and the structure, along with starting the interview questionnaire design to ensure that it aligns with the topic and the company's areas.

In the second phase, the collection of primary data from the interviews and a preliminary analysis of the literature are expected. It is essential to consider the time required for conducting the interviews, which is why it is one of the longest phases and requires the most flexibility.

In this phase, the articles and the comparison between the companies will be read, classified, and analyzed. The most significant challenge will be scheduling the interviews, which is why the option of using online resources has been decided.

A thematic matrix was created to get a clearer idea of the key concepts from the literature, showing what authors have in common (linking them not only with the literature but also with each other).

The third phase is part of the analysis and reflection of what has been obtained so far. The NVivo tool will be explored and tested here, as in other studies. However, since this is a request-based platform (which requires passing through several stages to use it for free), other platforms like ChatGPT and DeepSeek were considered and used, as they provide similar results with less detail.

In this phase, it was crucial to identify the similarities and differences between the companies' sizes and sectors, so tables and graphs will be employed to organize them visually.

It is important to note that preliminary justification or rejection of the hypotheses will begin in this phase.

As the name suggests, the penultimate phase will focus on discussing the results and analysis obtained in the previous phase. A second complete draft of the results and literature is expected to be ready by the end of the month.

This phase will be characterized by the term "findings," which will be interpreted by comparing them with previous studies and what has been learned from the literature. These findings will also be related to the implications for companies and future research.

Finally, the closure phase involves writing the conclusions, recommendations, and reviewing the entire thesis content multiple times. It will be a cycle of revision, adaptation, and conclusion. Without a doubt, the cohesion, coherence, and clarity of the work will be reviewed to ensure that ideas are as concise as possible without diminishing the value of the work.

Additionally, the key data obtained will be used to design a presentation, and preparation for the thesis defense will take place.

2.1. Literature Review

2.1.1 Cybersecurity Challenges for SMEs vs. Large Enterprises

Many studies on cybersecurity consistently highlight distinct challenges faced by small and medium-sized enterprises (SMEs) compared to large enterprises. Many authors, such as Vijayakumar and Ilangovan, say that SMEs are particularly vulnerable due to several inherent limitations.

First, limited financial resources constrain their ability to invest in advanced security infrastructure (Vijayakumar & Ilangovan, 2015:90). Furthermore, many SMEs lack in-house cybersecurity expertise, which often forces them to rely on external providers or generic security solutions that may not be fully tailored to their specific needs (Murphey, 2020:1). This dependency on third-party security solutions can leave gaps in their overall defense strategy.

Recent findings show that SMEs, despite their economic importance, often underestimate the scale of their exposure to cyber threats. According to Paulsen (2016:92), small businesses usually do not realise they are big targets, even though they represent about 99% of all companies and contribute significantly to employment and GDP globally. Additionally, studies have shown that the rapid evolution of cybercrime into an organised and highly profitable activity (sometimes referred to as "Crime as a Service") places SMEs in an even more vulnerable position due to their limited resilience capabilities (Manky, 2013: 9-10).

It is crucial to remember that, according to the World Bank (2019), SMEs constitute around 90% of total companies worldwide and create more than 50% of employment globally. In Spain, 99.8% of enterprises are SMEs, and 19% are in Catalonia. In other words, one out of five Spanish SMEs is located in Catalonia (Via Empresa, 2024). This highlights the importance of enhancing cyber resilience within this sector.

Moreover, challenges within SMEs are technical, human, and organisational. Studies such as Aschwanden et al. (2024) stress how employee behaviour and psychological biases often act as gateways for cyberattacks. Many SMEs fail to assign responsibility for cybersecurity behaviour to their staff, resulting in unaddressed vulnerabilities. The lack of awareness and insufficient training leads to risky behaviours, making internal threats (both accidental and intentional) one of the leading causes of data breaches (Sharton & Ansbach, 2020).

Another notable concern is the cybersecurity skills gap, particularly in Europe. Around 291,000 cybersecurity professionals are needed to meet demand (Murphey, 2020:1). This makes SMEs especially disadvantaged as they struggle to compete with larger firms for talent. It is therefore suggested that SMEs focus on training existing staff to be more security-conscious and consider internal role transitions for cybersecurity duties.

Larger enterprises, on the other hand, are generally said to possess dedicated cybersecurity teams and more substantial budgets to implement advanced, multi-layered security strategies (Mhlongo, van der Poll, & Sethibe, 2023). However, it is also discussed how their larger digital footprint and higher visibility make them attractive targets for sophisticated and highly coordinated cyberattacks (Epstein, 2023:33). With the attack surface continuously expanding due to AI, IoT, and cloud computing, the need for ongoing audits, incident response plans, and employee education is essential to maintain cyber resilience (Global Digital Trust Insights, 2025).

Despite increasing awareness, gaps in cyber resilience still exist across all company sizes. Only 2% of executives report having implemented resilience strategies in all necessary areas, and many still lack proper risk measurement systems or apparent involvement from CISOs in strategic planning (PwC, 2025:3). These organisational gaps, coupled with differences in regulatory compliance confidence between CEOs and CISOs, reveal a pressing need for more substantial alignment at the executive level (PwC, 2025:3).

Finally, cybersecurity should not be seen merely as a technical issue but as a multidisciplinary and cultural one. Craigen, Diakun-Thibault, and Purse (2014) argue that the lack of a comprehensive definition of cybersecurity hinders progress and cross-disciplinary collaboration. Chang (2012) also explains that cybersecurity is fundamentally an adversarial issue involving humans defending machines from other humans. It requires insights from fields beyond IT, such as psychology, management, and law.

Organisations, especially SMEs, should develop a cybersecurity culture (CSC) that integrates strategy, people, and technology to create a resilient digital infrastructure. This culture should be aligned with the organisation's overall values and involve all employees, not just the IT department (Corradini, 2020:74). An effective CSC starts with internal assessment, clear communication, and leadership commitment. Stanton

et al. (2017:24) state that fostering a "culture of security" through continuous employee training and well-defined access management policies can significantly reduce risks.

2.1.2 Theoretical Frameworks for Cybersecurity Management

The literature employs several theoretical perspectives to frame the discussion on cybersecurity management. These theories explain not just what businesses do but why they do it, and they are especially useful when comparing small and large companies.

Institutional Theory posits that organizations implement cybersecurity measures primarily in response to external pressures such as regulations, industry standards, and public expectations (DiMaggio et al., 2000). In other words, instead of acting only based on their own internal needs, businesses sometimes follow what others in their industry are doing to keep up or to look good in the public eye. In that sense, this theory helps us see how external forces like regulations or social norms shape internal decisions about digital security.

Complementing this view, the Resource-Based View (RBV) suggests that organizations with greater financial and technical resources (typically large enterprises) can develop and sustain more effective cybersecurity defenses than resource-constrained SMEs. This leads to companies (more typically SMEs) responding to incidents only after they happen instead of preventing them in the first place (Barney, 1991). This theory is essential because this thesis compares companies of different sizes and tries to understand how their resources affect their cybersecurity strategies.

The Technology Acceptance Model (TAM) further elaborates on how businesses adopt cybersecurity technologies by emphasizing the importance of perceived usefulness and ease of use (Davis, 1989). This is helpful when thinking about why some companies (mostly larger ones) quickly adopt new cybersecurity tech while others are slower.

Meanwhile, Organizational Culture Theory emphasizes that corporate culture plays a critical role in shaping cybersecurity awareness and employee behavior, which in turn affects the organization's overall security posture (Schein & Schein, 2017). This is especially useful when looking at how employees deal with cybersecurity, for instance, whether they follow policies, attend training, or even realize the risks

involved. A company's internal culture can significantly affect how seriously people take cybersecurity.

Finally, Risk Management Theory provides a structured approach to assessing and mitigating cybersecurity risks, offering a systematic framework for organizations to quantify and address potential vulnerabilities; this includes planning, training employees, and setting up policies that help avoid or manage damage from attacks. (Kaplan, Haimes, & Garrick, 2021). In other words, it is about how organizations react to uncertainty.

While the literature employs a variety of theories, this study primarily draws on the Resource-Based View and Organizational Culture Theory. The RBV was chosen because it aligns well with the comparative nature of the research, highlighting the differential capacities of SMEs and large enterprises. In parallel, organizational culture theory offers a valuable lens to understand how internal practices and the overall corporate image contribute to mitigating the real-world impacts of cyberattacks. This study will also consider the TAM and risk management theory, making its contribution less than the first two mentioned. Nevertheless, these frameworks were selected for their relevance and depth in addressing the core objectives of this study.

2.1.3. Management of Cyber Risks

Managing cyber risks requires a proactive and multilayered approach, integrating technological and organizational strategies. In other words, it means understanding the technical side of cybersecurity and the social and organizational elements that influence how a company reacts to threats.

One of the foundational elements of cybersecurity risk management is compliance with industry regulations, such as the General Data Protection Regulation (GDPR) and ISO/IEC 27001, which establish best practices for data protection and security (ISO/IEC 27001, 2013). However, it is also important to understand that cybersecurity is not just a technical issue but a multidisciplinary challenge.

Craigen, Diakun-Thibault, and Purse (2014:13) explained that the lack of a clear and widely accepted definition of cybersecurity has slowed progress by reinforcing a narrow technical focus and separating related disciplines that should collaborate.

Chang (2012) argued that because cybersecurity is essentially adversarial, in other words, humans defending machines against other humans using machines, it must be addressed through collaboration between fields like computer science, engineering, law, psychology, and business. Organizations, therefore, need to go beyond regulations and technical solutions by creating a culture of cybersecurity that is part of the broader organizational culture (Corradini, 2020:77).

Cybersecurity Culture (CSC) must be actively developed through a strategy that includes people, technology, and process alignment. Corradini (2020) emphasized the need for internal assessment, top management commitment, and clear communication to help staff understand and follow security practices. In this context, cybersecurity becomes everyone's responsibility, not just the IT department's.

The current threat landscape is also expanding due to technologies like AI, cloud computing, and IoT, making cyber resilience essential. Still, a report from PwC (2025) shows significant gaps between awareness and implementation. For example, fewer than half of executives report that their CISOs are fully involved in strategy, and only 15% measure the financial impact of cyber risks. These gaps can increase vulnerabilities and hinder the development of strong cyber risk frameworks.

A major concern for many organizations is insider threats. These threats can come from employees or partners who are either negligent or intentionally harmful. Sharton and Ansbach (2020) noted that some insiders act deliberately, while others may unknowingly help external attackers by clicking on malicious links or exposing credentials. Similarly, Zielinski (2019:1) reported that 55% of enterprises experienced a data breach within a year, and nearly half were caused by internal actions.

To reduce this risk, companies should follow the principle of least privilege, giving employees access only to the information they need for their jobs (Zielinski, 2019). Regular employee training is also essential, as humans are often the weakest link. Stanton, Ernst, and Janik (2017) suggested that organizations should promote a "culture of security" through clear policies, regular training, and consistent enforcement.

Small and medium-sized enterprises (SMEs) face special challenges. Paulsen (2016:93) noted that SMEs play a significant role in economic growth but often lack resources and cybersecurity expertise. Still, SMEs can build flexible cybersecurity strategies and even a culture around it. According to Mhlongo, van der Poll, and

Sethibe (2023), SMEs struggle with limited access to training, IoT complexity, and management inexperience. This makes their cybersecurity management more difficult, but not impossible, if they apply achievable solutions like cloud-based protections and commit to staff training.

Another problem is the growing cybersecurity skills gap. Murphey (2020) emphasized that many organizations must fill hundreds of thousands of cybersecurity positions, especially in Europe. One solution is to retrain existing employees who understand the company's IT systems, rather than only looking outside for talent.

In addition, cybercrime has become a well-structured and organized business, with its own hierarchy and business models like "Crime as a Service" (Manky, 2013). Fighting it requires international cooperation, continuous audits, and a layered defense strategy. Companies also need incident response plans and partnerships with cybersecurity experts.

Finally, managing cyber risk also includes using insurance and understanding the organization's vulnerabilities. Risk assessment frameworks like those introduced by Kaplan, Haimes, & Garrick (2021) offer structured ways to measure exposure.

In conclusion, effective cyber risk management goes beyond technical tools and compliance. It requires an interdisciplinary approach, strong leadership, staff training, clear policies, and a cybersecurity culture that supports awareness and shared responsibility.

2.1.4. Cybersecurity in Management

Cybersecurity is no longer solely an IT concern but a strategic business issue that requires top management involvement. As Fisher, Porod, and Peterson (2021) note, effective cybersecurity management demands that corporate governance and decision-making processes fully align with security practices.

Similarly, Singer and Pratt (2016) and Epstein (2023) argue that cybersecurity must be integrated into the overall business strategy through active involvement from executives and board members. Epstein (2023) contends explicitly that organizations should regard cybersecurity not just as a cost, but as a crucial component of operational resilience.

From a definitional standpoint, Craigen, Diakun-Thibault, and Purse (2014:13) assert that "the absence of a concise, broadly acceptable definition that captures the multidimensionality of cybersecurity impedes technological and scientific advances". They emphasize that this narrow, predominantly technical view fractures disciplines that should work together to resolve complex challenges.

Moreover, the dynamic nature of today's cyber threat landscape (fueled by advances in artificial intelligence, connected devices, and cloud technologies) requires that businesses continuously update their defenses. These findings reveal that even large organizations with dedicated cybersecurity teams are not immune to sophisticated, coordinated attacks due to their extensive digital footprints (Epstein, 2023).

Employee behavior is another critical factor. Zielinski (2019: 2) remarked, "Hackers have learned that it's much easier to hack people than to hack technology." This is supported by research from Sharton and Ansbach (2020), which underscores that insider threats, whether due to negligence or malicious intent, pose significant risks. Consequently, a "culture of security" is essential; organizations must ensure that access to sensitive data is limited to those who require it and that employees receive continuous training (Zielinski, 2019; Stanton et al., 2017).

The cybersecurity skills gap further complicates management challenges. This shortage necessitates internal investments in training and the potential reallocation of existing personnel, ensuring that managers understand cybersecurity's technical and strategic aspects. Effective leadership can bridge the gap between technology and organizational behavior, fostering a resilient and adaptive cybersecurity culture (Triplett, 2022: 35).

Finally, the evolution of cybercrime into a highly organized business model, often described as "Crime as a Service" (Manky, 2013), accentuates the need for businesses to adopt a multi-layered defense strategy. This strategy should involve regular audits of digital assets, proactive incident response planning, and, importantly, the integration of cybersecurity into the company's broader risk management framework. As highlighted by Corradini (2020:11), embedding cybersecurity into the organizational culture helps maintain trust, build resilience, and ultimately ensure long-term business success.

In summary, cybersecurity management today requires an interdisciplinary approach that follows regulatory requirements, adopts advanced technological solutions, and emphasizes a strong organizational culture and leadership commitment. This integrated approach is vital for SMEs and large corporations to defend against increasingly complex cyber threats.

2.1.5 Common Thread in The Studies

Table 2. Common Thread in The Studies.

COMMON THEME	**DESCRIPTION**	**SUPPORTING STUDIES**
Evolving Cyber Threat Landscape	Cybercriminals continuously adapt their tactics and technologies, creating an ever-changing threat environment.	Singer & Pratt (2016); Epstein (2023)
Vulnerability of SMEs	SMEs are particularly vulnerable due to limited financial resources, insufficient in-house expertise, and reliance on third-party security solutions.	Vijayakumar & Ilangovan (2015); Amrin (2014)
Challenges for Large Enterprises	Despite having dedicated cybersecurity teams, large enterprises face complex and sophisticated attacks due to their extensive digital footprint and high visibility.	Epstein (2023)
Importance of Human Factors	Human error, inadequate training, and weak organizational culture are critical factors that can undermine cybersecurity defenses.	Przymus et al. (2024); Fisher et al. (2021); Schein, & Schein, (2017).

Comprehensive Risk Management	Effective cybersecurity requires a proactive, multi-layered risk management approach, including compliance with international standards and the integration of IT with broader organizational policies.	Kaplan, Haimes, & Garrick, (2021); Dirksen (2022); Santos (2024)

Source: Author's own elaboration from the different publications.

A literature review reveals a persistent theme: cyber threats are continuously evolving, and so must the strategies to counter them. Studies agree that cybercriminals continuously adapt their techniques, leveraging technological advancements to exploit vulnerabilities (Manky, 2013:11-12). The introduction of artificial intelligence (AI) in cybersecurity has been a double-edged sword, with businesses utilizing AI for fraud detection. At the same time, cybercriminals weaponize it for sophisticated attacks (Singer & Pratt, 2016).

SMEs are frequently highlighted as particularly vulnerable due to their limited financial and technical resources, which restrict their ability to implement robust cybersecurity measures (Vijayakumar & Ilangovan, 2015:90). In contrast, large enterprises, despite possessing dedicated cybersecurity teams, face a higher likelihood of targeted, complex attacks owing to their extensive digital infrastructures and greater public visibility (Epstein, 2023; Singer & Pratt, 2016).

Studies further emphasize the role of human error in cyber incidents. Researchers argue that organizations must invest in cybersecurity awareness and training programs, as social engineering attacks continue to be one of the most successful methods of breaching corporate security (Przymus et al., 2024). The impact of cyberattacks goes beyond financial losses; reputational damage can significantly affect consumer trust and business sustainability (PwC, 2020).

The concept of cybercrime as a service further underlines the democratization of hacking tools, thereby intensifying the threat landscape across sectors. In essence, the common thread across these studies is the urgent need for organizations of all sizes to adopt agile and adaptive cybersecurity measures that address both technical vulnerabilities and human factors (Przymus et al., 2024:420).

2.1.6. Gaps Of Study

Despite the growing body of research on cybersecurity risk management, significant gaps remain for further investigation. First, much of the existing literature has concentrated on technological solutions, with limited emphasis on strategic and organizational dimensions of cybersecurity management. For example, Al-Somali et al. (2024) indicate that research on SMEs' cybersecurity strategies rarely extends beyond implementing technical measures.

Second, there is a notable lack of comparative studies between SMEs and large enterprises, especially within specific regions such as Catalonia. Chidukwani et al. (2022:12) emphasize that while individual cybersecurity challenges have been documented for different organizational sizes, direct comparisons in localized settings are scarce, limiting the understanding of context-specific vulnerabilities and best practices.

Finally, current studies explore the human element in cybersecurity management. Critical aspects such as HR policies and organizational behavior (essential for fostering a robust cybersecurity culture) receive insufficient attention (Fisher et al., 2021).

These gaps highlight the need for a more holistic research approach that integrates technological, organizational, and human factors. This approach would thereby provide a comprehensive understanding of cybersecurity management across various enterprise sizes and contexts.

2.2. Methodology and approach of this study

This study combines the analysis of 25 past case studies done in this field of work, which expose a clear case and look for common themes, hypotheses, and solutions, thereby connecting patterns. Another source of primary data was collected from twelve interviews to get a personalized view of the Catalonia case and compare it to what past resources explained and obtained as a result. For that, the approach of this study was divided into four steps.

The first step is titled the standard literature review. It was guided by the study of Tranfield, Denyer, and Smart (2003), which was mentioned by the study of Alahmari and Duncan (2020), which was chosen as the main research to follow for this thesis work.

The authors mention three stages for the literature analysis: planning the review (defining the scope of research, in this case, cyberattacks, and relevant keywords like "risk management" or "SMEs"), conducting the review (databases and coding the data using software, in their case, NVivo), and reporting the findings (synthesizing the key discoveries).

Although this thesis draws inspiration from their methodology, it does not conduct a systematic literature review due to the complexity of the process and resource limitations. Only scientific articles of case studies were considered in this review, leaving the theoretical reviews and approaches for contextualization and a base of knowledge for this body of work. A total of 25 publications were analyzed.

The traditional method of selecting articles for this thesis was used. In other words, articles were chosen based on their frequent citation across a variety of trusted and verified sources. These articles were chosen for their established credibility, demonstrated by their consistent citation within the academic community. Additionally, studies were prioritized based on their valuable contributions to the field, ensuring their relevance to this research.

Ultimately, only the most pertinent articles aligning with trustworthiness and contributions to the field were included. The key point in this step is to recognize patterns, tendencies, and breaches in what has currently been studied in this field. This step was key to gaining a deeper understanding of the field.

Due to the impossibility of using the NVivo platform, a combination of two software tools (ChatGPT and DeepSeek) was chosen instead to extract a more complete and well-rounded analysis than would have been possible using just one of them.

They helped identify the main themes, hypotheses, and proposed solutions in the 25 articles. Afterwards, a table was created to track which hypotheses and solutions were discussed in each publication. This visual overview allowed for a clearer understanding of trends and patterns. Based on this, a Hypothesis-Solution Matrix was developed, showing how often each solution was linked to a specific hypothesis across the reviewed studies.

It was done via a prompt that specified the table needed. In both software, a document with the list of the articles and the option to reason before sending was clicked.

During this process, some limitations were observed in the tools themselves. ChatGPT, for instance (when using the free version), has a daily limit for generating detailed responses, sending multimedia files (with a maximum of three files allowed), or even limitations with accessing the latest version. DeepSeek allows more multimedia uploads (up to 50 files at the time of the study), but it limits chat interactions.

Both platforms tend to produce very generalized analyses, which require manual content and review expansion, as they sometimes make errors or fabricate data. Sometimes, it is necessary to give precise instructions, but even with detailed prompts, the tools can get "overwhelmed" and fail to retain the information. Also, especially in the case of DeepSeek, users may experience issues depending on the platform's server load, as it occasionally becomes unresponsive due to high traffic.

The second step was to interview the company representatives. Eight semi-structured interviews were conducted with company representatives to collect this data, in a face-to-face manner (with the exception of one interview, which was done online due to the circumstances and impossibilities of aligning schedules), to allow in-depth exploration of the answers between the questions.

Then it was decided to contact professionals in the field of cybersecurity to get a more in-depth and ongoing view on the matter. For this, a different set of guidelines was used.

The interviewees showed different opinions when asked if they could be recorded. Only five out of twelve agreed to the filming, transcription, and direct quotation of their answers; around 58% of the participants showed discomfort and disagreement with this step, and therefore, the interviews' data were collected by hand. This may be due to the uncertainty of the usage of the data; it was not perceived as a personal problem, but from a general point of view. This is a clear sign that in today's standards, privacy is valued, and therefore, even if it is subconscious, the interviewees made a clear statement about cybersecurity.

Interestingly, the ones that asked not to be recorded followed a calmer, looser, and unstructured interview. Making their answers as detailed as they called to be necessary, and no signs of "retention" were perceived. On the other hand, the ones that followed a more academic tone made their point and opinion heard. However, once the recording stopped and various informal conversations occurred, more

information and their underlying opinion were clearly shown. Nevertheless, all was respected and followed on a case-by-case basis.

One thing to notice is that the interviews with the more knowledgeable in this area of work (cyber professionals) were a lot denser and longer. The passion that this group showed towards their answers and the need to not only answer but also make sure they were understood was noticeable.

Due to this work's challenge, the interviewees represent all Catalan companies. Catalonia was chosen as the focus location of this thesis work because of its proximity and the interest in relying on the information found, while that being the reality presented. Changes between SMEs and larger enterprises were kept to a minimum, only when necessary to keep a standardization process between sizes, sectors, and participants. Context-specific responses were expected.

For this step, it was crucial to truly understand the key to the theoretical part of this work to connect it fully with the theories and the hypotheses. Therefore, the questions were asked in a way that provided a clear road to answering each hypothesis. Another thread was the comparative analysis between each enterprise and its size, considering the patterns, differences, and commonalities. The departmental roles and organizational culture played a massive part in this process.

Lastly, there is no need to mention the ethical considerations that were put into practice in this study. To ensure transparency and ethical and communicational openness, all participants were asked about their wishes for visibility in this report. They were asked for their consent to take part in this study, outlining its purpose, data confidentiality, and their right to withdraw from this process at any stage. The interviewees chose to stay anonymous and were treated as such in this thesis work, having their identities preserved in confidentiality, and were only reported when talking about the findings.

Taking this approach into account will give this study a chance to truly understand the framework of companies' daily adaptations to cybercrime. Although this document focuses on Catalan enterprises, the overall gain from this thesis will help understand this matter from a broader point of view.

2.2.1. The Sample

The literature selection forms part of the primary selection process. As mentioned at the beginning, 25 case studies were selected and used to update this line of work. Only trusted databases such as Scopus, IEEE, and SpringerLink were used, limiting the publication data of work to those which were published between 2015 and 2024. This was done to get the most up-to-date data possible.

The selection process involved a first review analysis, which selected only empirical studies that focused on cybersecurity risk management in SMEs and large enterprises. Studies were excluded if they lacked an empirical methodology or focused on non-business-related areas.

The company interviews also form part of the primary data group[2]. Eight companies in Catalonia were chosen to represent both the SME and Larger enterprise business categories. This was not an easy selection due to the magnitude of studies done in this field. The idea of focusing and distributing the comparison differently was brought up many times in the study, and it consists of a gap in this theme. In the end, it was decided to compare smaller and larger-sized companies due to the visual evidence of differences they both have and the variability of challenges they present.

The companies were deliberately chosen to reflect diverse sectors and their behavior within the sizes and areas. The areas selected were IT due to the expertise in cybersecurity and continuous work with the digitalization of the enterprise, standard workers to get to know what they implement internally to their employees and externally to the clients, and managerial or higher departments to review if they see an impact of this fraud on their daily work and to see if the chosen strategies to mitigate or prevent these attacks are fully understood and implemented. This diversity was considered important, as it was assumed that IT professionals would generally have greater knowledge about cybersecurity compared to those in other areas.

Both of these components are considered a basic base for a degree thesis work similar to this one but even more so in this specific case due to the nature of exportation of practical knowledge data in this subject; therefore, this makes this an untouchable step for the complete analysis and understanding of the practical cases and the interviews.

[2] Please view the Appendix for further information about the interviewees and interviews.

2.2.2. The Variables

For this study, it was decided to separate the variables between independent and dependent variables, as most other studies do.

Given the qualitative nature of the study, variables were defined conceptually rather than quantitatively; therefore, because this thesis will not be extracting numerical data, the variables and the discussion and decision of these are of primary need.

Without further introduction, the independent variable is the company size (SMEs versus larger enterprises). The dependent variables are the perception of cybercrime[3], the strategies employed[4], the impact of cybercrime[5], and the adoption of technology[6]. The last two were asked about the challenges perceived, the will, openness, and existence of training programs, and their view (attitude) towards these kinds of attacks (whether they agreed which one had more sophisticated attacks, or which one was the most targeted).

As mentioned above, the independent variable in this study is the company's size, which has been chosen due to the nature and curiosity of a comparative approach between small and medium-sized enterprises (SMEs) and large corporations. This comparative focus is particularly relevant because limited work has been done on comparing cybersecurity practices between these two groups, and even less so with a specific focus on Catalan companies. The division by company size is expected to highlight differences in resources, strategies, and the overall cybersecurity culture, which are critical factors in understanding how organizations adapt to emerging cyber threats.

Moreover, the dependent variables in this research have been selected based on past research and references in the field. Previous studies have consistently shown that the perception and awareness of cyber risks, the measures taken to secure information, and the resulting impact of cyber incidents vary significantly according to an organization's resources and culture (Vijayakumar & Ilangovan, 2015; Triplett, 2022). Moreover, the degree of technology adoption, particularly innovative solutions such as artificial intelligence, has been identified as a key differentiator between

[3] The awareness and understanding of these types of risk.
[4] The measures the companies take to prevent and mitigate these attacks or the solutions they perceive as the better option.
[5] How the damages are portrayed internally and externally.
[6] The easy adaptation and flexibility to more technological tools such as the use of AI.

organizations with robust cybersecurity postures and those that struggle to protect their digital assets.

By focusing on these dependent variables, this study aims to build on earlier work while providing new insights into the unique challenges and opportunities faced by companies in Catalonia and beyond.

2.2.3. The Hypothesis

H1: Larger companies have a higher perception and awareness of cybercrime than SMEs.

First, it is hypothesized that larger companies have a higher perception and awareness of cybercrime compared to SMEs. In other words, this first hypothesis works with the independent variable, company size, and the perception of crime (dependent variable).

This assumption is supported by the Resource-Based View (RBV), which explains that larger companies have more financial and technical resources to invest in specialized cybersecurity training and expertise (Barney, 1991). Additionally, Organizational Culture Theory suggests that companies with more developed cultures are better at disseminating security knowledge across all levels of the organization (Schein & Schein, 2017). Consequently, larger enterprises' enhanced resources and culture are expected to lead to a greater overall awareness of cyber threats.

H2: Larger companies implement more comprehensive cybersecurity strategies than SMEs.

Secondly, the study hypothesizes that large companies implement more comprehensive cybersecurity strategies than SMEs.

According to the RBV (Barney, 1991), larger companies can afford to invest in advanced, multi-layered cybersecurity defenses because of their greater resource base. Additionally, Risk Management Theory (Kaplan & Garrick, 1981) provides a structured approach to evaluating and mitigating risks, which larger organizations are better positioned to implement. This combination supports the idea that large enterprises can adopt more sophisticated cybersecurity measures than SMEs. In other words, large companies are anticipated to adopt more sophisticated and

proactive strategies compared to SMEs, which typically rely on simpler, less formalized approaches.

H3: SMEs experience a more severe impact from cyberattacks than large companies.

This is likely because SMEs, due to limited resources and fewer specialized personnel, are generally less prepared to respond to and recover from cyber incidents. This was studied again in the RBV theory, which indicates that with limited financial resources and fewer technical experts, SMEs are less equipped to handle the aftermath of a cyberattack (RBV; Barney, 1991). In addition, Risk Management Theory (Kaplan, Haimes, & Garrick, 2021) indicates that without effective risk measurement and incident response frameworks, even moderate cyberattacks can result in high operational and reputational damage.

Therefore, this hypothesis posits that SMEs' relatively lower resilience leads to a greater negative impact when a cyberattack occurs.

H4: Large companies are more likely to adopt advanced cybersecurity technologies like artificial intelligence than SMEs.

Finally, the study hypothesizes that large companies are more likely to adopt advanced cybersecurity technologies, such as artificial intelligence, than SMEs (company size vs. technology adoption).

The Technology Acceptance Model (TAM) explains that adopting new technology is driven by perceived usefulness and ease of use (Davis, 1989). Larger organizations, by their ample resources and more sophisticated infrastructures, are better positioned to evaluate, adopt, and continuously update advanced technologies, as reinforced by the RBV (Barney, 1991).

In summary, this study's hypotheses are based on the idea that a company's size can shape how it manages cybersecurity. From the theoretical framework, we can conclude that bigger companies usually have more resources, stronger internal structures, and clearer strategies, often leading to higher awareness of cyber risks, better prevention methods, and more advanced tech adoption. On the other hand, SMEs are said to often face more challenges because of their lack of resources and weaker risk management systems compared to larger enterprises.

These ideas are backed by the key theories selected for this thesis publication, like the Resource-Based View, which explains how resources influence a company's capabilities, and Organizational Culture Theory, which highlights how internal values and practices affect cybersecurity behavior. Also, the Technology Acceptance Model helps explain how companies adopt new tech based on how useful and easy it seems, and Risk Management Theory shows how systematic planning can reduce cyber risks. Together, these theories offer a solid base for the research and help explain why company size matters regarding cybersecurity.

2.3 Results and Discussion

To better structure the results section, this study distinguishes between two types of data: quantitative and qualitative. The results from the article analysis are considered quantitative because they present measurable data such as percentages, frequencies of incidents, or trends in cybersecurity practices. These articles were used to build a problem-solution matrix and identify graph patterns, reflecting a numerical, trend-focused approach. With the help of the two AI software programs, key patterns were identified.

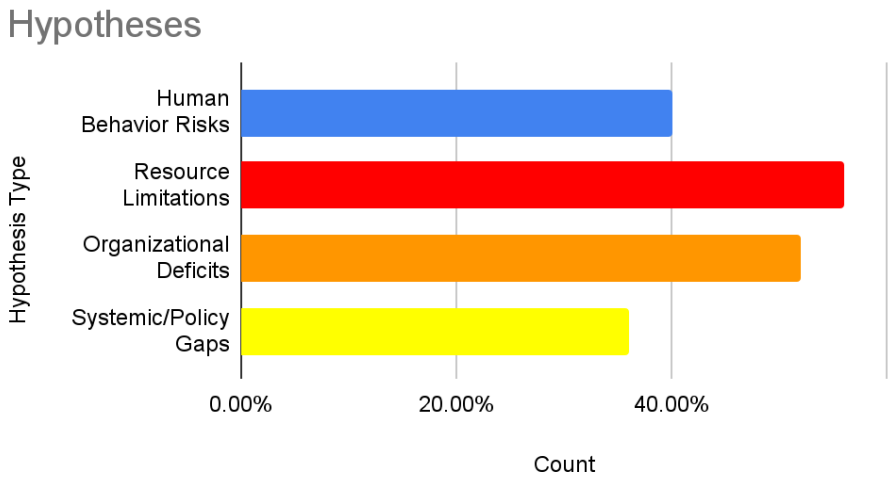
On the other hand, the interview results are qualitative, as they rely on the personal opinions and experiences of the interviewees. The open-ended answers explored how individuals perceive and respond to cyber threats inside their companies. These insights helped provide a more human, detailed view that complements the statistical overview. Dividing the findings this way allows the study to compare general trends with real workplace experiences and draw broad and specific conclusions.

2.3.1 Quantitative Results: Analysis of Case Studies

From those twenty-five publications[7], we can extract a few important conclusions.

[7] Please refer to the Appendix to view the selection.

Figure 1. Most Frequent Hypotheses from the Publications Analyzed.



Source: Author's own elaboration from the 25 articles analyzed.

After reviewing the hypotheses presented in the selected studies, they can be grouped into four main categories. The horizontal bar chart shows that resource limitations are the most frequently mentioned hypothesis. This idea highlights that smaller companies are generally more exposed to cyber threats due to their limited budgets and internal resources. In contrast, larger companies often have more financial flexibility and can allocate part of their capital to manage better or reduce cyber risks.

One of the main articles by Watad, Washah, and Perez (2018) explains that many small business managers do not consider security tools crucial for their operations. They argue that SMEs often have tight budgets and lack well-trained staff, so they rely on basic tools like antivirus software and firewalls. This leaves them at a higher risk of cyberattacks, mainly due to cost issues and a lack of awareness.

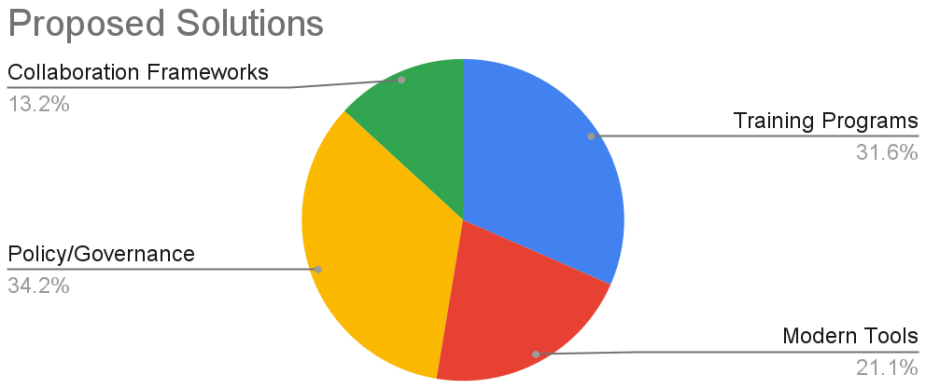
A study by Adriko and Nurse (2024) offers a different perspective, adding that SMEs struggle with organizational problems like missing cyber insurance policies. They argue that businesses cannot manage risks properly without clear rules or trained leaders. This gap exposes SMEs to attacks, even if they have some tools. Research shows that organizational defects (like bad leadership and weak policies) are the second biggest problem for SMEs after limited budgets.

Authors such as Roberts (2021) and Osawaru (2024) emphasize that many cybersecurity problems are caused by small, routine mistakes made by employees.

This is another highly discussed category: human behavior risks, which appears in ten of the studies. These errors often go unnoticed but can be exploited by cybercriminals, as workers are usually unaware of how their actions might lead to security breaches. For example, Buehrly-Harris (2024:17) shows that limited user knowledge significantly increases the risk of cyber incidents, highlighting the need for targeted training programs.

The problem with cybersecurity hypotheses is that it is rare for there to be a single question. Instead, they often involve multiple overlapping factors, requiring researchers to address a mix of hypotheses like human error, resource limits, and organizational gaps. This was not a disadvantage; it was just a note to take notice of because this overlap means that effective cybersecurity research must analyze interconnected hypotheses, not isolate them.

Figure 2. Most Frequent Proposed Solutions by the Publications analyzed.



Source: Author's own elaboration from the 25 articles analyzed.

As shown in the graph, when grouping the solutions suggested by the authors, four categories emerge: training programs, policy arrangements, collaboration frameworks, and modern tools.

Surprisingly, the publications showed a bias towards Policy/Governance solutions. These solutions are based on creating or improving rules, leadership structures, and compliance systems. For example, Al-Somali et al. (2024) urge adopting frameworks like ISO 27001 to standardize rules.

Adriko and Nurse (2024) offer a different perspective on reviewing cybersecurity, cyber insurance, and SMEs research. Their work suggests that cyber insurance could provide SMEs with financial protection and expert advice. However, the uptake is low because many business owners do not understand the risks or insurance policies. They stress the importance of clearer, simpler policies and better government support to boost confidence in these measures.

The graph also highlights the implementation of training programs aimed at increasing employee awareness and helping staff recognise and prevent cyber threats. The literature strongly supports this idea, especially by Buehrly-Harris (2024), who argues that making cybercrime risks more visible within the company environment can significantly improve prevention.

Studies also examine the use of new technologies. Rawindaran et al. (2022) explored how Welsh SMEs use smart technologies, like machine learning tools, to defend against cybercrime. Their findings show that most SMEs are not very familiar with these advanced tools (only about 30% had any real knowledge of them) (Rawindaran et al. 2022: 1). This low level of understanding, along with factors like company size and education level, plays a significant role in whether SMEs adopt better security measures.

On the other hand, collaboration frameworks were the least mentioned solution, accounting for only 13.2% of the total suggestions across the reviewed studies. Singh and Abu Bakar's (2019) study proposes a model to coordinate efforts among businesses, regulators, and security experts, stressing that collaboration is key.

Similar to the hypotheses, the solutions more often than not propose more than one group of solutions to mitigate cyber risks. Therefore, making a whole mix of the four to represent the best solution. Research by Chidukwani, Zander, and Koutsakis (2022), as well as studies by Rawindaran, Jayal, and Prakash, E. (2022), consistently point out that employee training, strong leadership, and a regular update and incorporation of modern tools are critical for effective cybersecurity.

Lastly, Al-Somali et al. (2024:18) note that robust cybersecurity systems, backed by an engaged organizational culture, protect a business and improve overall performance.

Figure 3. Hypothesis-Solution Matrix from the Publications Analyzed.

Hypothesis-Solution Matrix				
Hypothesis \ Solution	Training Programs (T)	Modern Tools (M)	Policy/Governance1 (P)	Collaboration Frameworks (C)
Systemic Policy Gaps (S)	1	3	7	3
Organizational Defects (O)	5	1	11	4
Resource Limits (R)	4	7	8	3
Human Error (H)	10	3	2	2

Source: Author's own elaboration from the 25 articles analyzed.

The final graph illustrates the connection between the identified hypotheses and their corresponding solutions, using a colour scale to indicate how frequently each link was mentioned. As shown in the image, red represents the highest number of mentions, gradually decreasing to green, which indicates the least frequent connections.

This table can be interpreted as follows: Eleven studies link Organizational Deficit risks to Policy/Governance solutions. In other words, these articles suggest that the most effective way to address problems such as bad leadership or unclear rules in a cybersecurity manner is through the creation of clear policies, pointing to a strong belief that internal rules and structures need to improve.

The high number of articles connecting these issues (three out of four problems where this solution was the most mentioned) reflects a common concern about weak or unclear structures inside companies. This connects with Hypothesis 2, about the strategies employed, and supports Risk Management Theory, since many studies focused on how policies help reduce vulnerabilities.

Human Error was most often linked to Training Programs (10 times), which supports the idea that improving cybersecurity starts with education. Authors like Bada and Nurse (2019:406) also suggest this last point: city-level educational programs could bridge the gap between academic insights and practical measures, making cybersecurity more accessible for SMEs.

This ties directly into Institutional Theory, which explains how external pressures can push businesses to adopt better cybersecurity practices. The emphasis on training also reflects the importance of organisational culture, as defined by Schein and Schein (2017), since these practices rely heavily on how companies shape employee behaviour and responsibility.

All these studies reveal some common themes: SMEs face major hurdles like limited resources, low cybersecurity awareness, and a shortage of trained professionals. Although large companies generally have the advantage of bigger budgets and more sophisticated security systems, they too must continually update their strategies to keep pace with evolving threats. In both cases, having strong leadership, encouraging a culture of continuous training, and receiving adequate support (whether from within the company or via government initiatives) are key to reducing risks and safeguarding information. These findings align with the hypotheses and support using this research's resource-based view and organizational culture theory.

2.3.2 Qualitative Results: Analysis of Interviews

Table 3. Key Questions by Themes and Linked Hypotheses Asked.

INTERVIEW QUESTION/ SECTION	**RELATED DEPENDENT VARIABLE & HYPOTHESIS**	**LINKED THEORIES**	**PURPOSE/ OBJECTIVE**
Cybersecurity Professionals			
Q3: "Based on your experience, what are the main cybersecurity challenges companies face?"	H2: Larger companies use more comprehensive strategies; H3: SMEs experience greater impacts	RBV; Risk Management Theory	To explore overall challenges and see if strategies differ by company size
Q4: "Do you observe significant differences in vulnerability and response between SMEs and large companies?"	H1: Perception differences; H2: Differences in strategies; H3: Differential impacts	RBV; Organizational Culture Theory; Risk Management Theory	To compare perceptions and responses between SMEs and larger enterprises

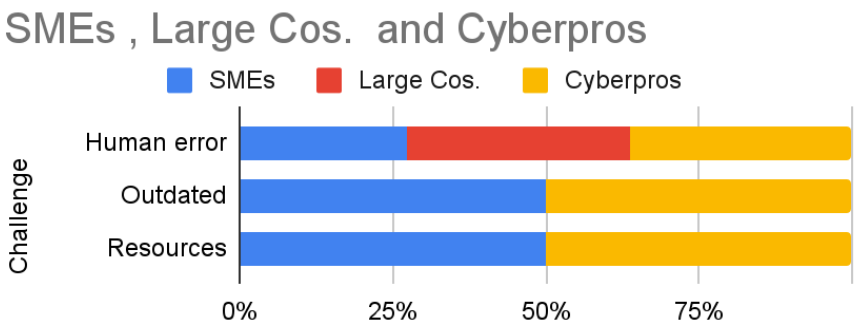
Q7: “How does the adoption of new technologies (e.g., cloud, AI) influence the effectiveness of cybersecurity measures?”	H4: Large companies are more likely to adopt advanced technologies	Technology Acceptance Model; RBV	To assess the role of technological innovation in strengthening cybersecurity
Q9: “From your perspective, how important are formal risk assessment and incident response plans in a company’s security?”	H2: Strategies employed; H3: Impact reduction	Risk Management Theory; RBV	To determine the significance of structured risk management in mitigating impacts
SME Representatives			
Q6: “What cybersecurity resources does your company allocate (staff, budget, technology)?”	H1: Perception of risk; H2: Strategies employed	RBV	To gauge whether limited resources in SMEs affect their awareness and measures
Q8: “Do you think these resources are sufficient to face current cyber risks? Why?”	H3: Greater impact on SMEs	Risk Management Theory; RBV	To identify gaps in resource allocation that may lead to higher vulnerability
Large Enterprise Representatives			
Q7: “If you were the CEO, how would you distribute cybersecurity resources in your large company?”	H2: Strategies employed; H4: Adoption of technology	RBV; Technology Acceptance Model	To analyze strategic allocation and its link to adopting advanced security tools

Q9: “How do you think resource allocation (budget, staff, tech) influences your company’s cybersecurity posture?”	H2: Strategies employed; H3: Impact reduction	RBV; Risk Management Theory	To explore how well-resourced companies manage risk and mitigate threats
Shared Questions (Both Groups Related to HR & Culture)			
“How is cybersecurity integrated into your company’s culture?”	H1: Perception of cybercrime; H2: Strategies employed	Organizational Culture Theory	To understand the role of internal culture in fostering cybersecurity awareness and proactive practices
“What kind of cybersecurity training and interdepartmental collaborations exist in your organization?”	H1: Perception improvement; H2: Strategies alignment	Organizational Culture Theory; Risk Management Theory	To assess the impact of training and collaboration on reducing human-related vulnerabilities

Source: Own Author’s elaboration.

The table aligns each question with one or more of the study’s hypotheses and theories. For example, questions about resource allocation and risk management (H2 and H3) are linked to theories like the Resource-Based View and Risk Management Theory and so, each interview is also connected to one or more theories from the ones studied in this Degree Thesis work.

Figure 4. Key Perceived Challenges from the Answers of the Interviews.



Source: Own Author's elaboration from the responses extracted from the Interviews.

This graph represents the key challenges the interviewees thought each of the This graph represents the key challenges the interviewees thought each situation could describe. For instance, the larger companies were highly concerned that human error is the main (and only) challenge within cybersecurity.

As seen above, the three groups mentioned human error as an important matter in the cybersecurity field. This supports Hypothesis 2 (H2), which assumes differences in cybersecurity strategies between companies of different sizes. It also aligns well with Organizational Culture Theory since employee behavior and internal culture play a significant role in security outcomes.

Cyber professionals also support this idea, emphasizing that attackers often target the individual rather than the whole company. Larger enterprises addressed this by focusing on training and simulations, showing a clear proactive approach.

The representatives of the SMEs acknowledged this but were highly more concerned about a cyberattack happening because of resource limitations or their lack of new technology[8] than because of human error, which aligns with the Resource-Based View (Barney, 1991). In response, most suggested that outsourcing and tailored training would be their go-to strategy if they had more financial control. These findings also align with Risk Management Theory, as SMEs show reactive behavior, while large firms act more proactively.

Cyber Professionals confirmed that new tools like AI and cloud services offer both opportunities and vulnerabilities and showed better adoption within larger

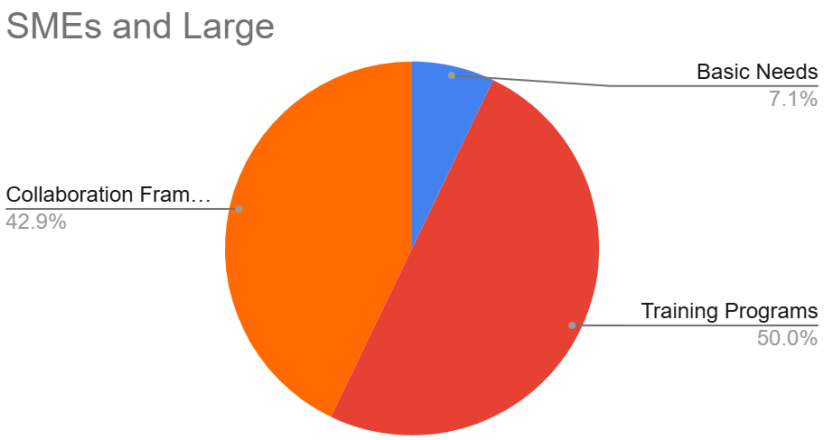
[8] This was linked with the reasoning mentioned before (resource limitations).

companies, mainly because they have the capacity to understand and afford them. These answers support the adoption of technology (Q7), Hypothesis 4, and TAM.

In contrast, SMEs often saw these tools as confusing or unnecessary, suggesting a low perceived usefulness and ease of use, two key ideas from the Technology Acceptance Model.

While larger companies have already integrated tools supported by in-house departments, SMEs rely on external providers. They are often unaware of what tools are being used or how. This reinforces H1, as larger companies showed a higher awareness of risks. It also supports H2, since their strategies were clearly more formalized and integrated, and H3, since SMEs were described as more affected when breaches occur due to their slow or reactive response.

Figure 5. Solutions Mentioned by the Representatives of the Companies.



Source: Own Author's elaboration from the responses extracted from the Interviews.

According to the interviewees, the pie chart shows the preferred types of cybersecurity solutions. The most mentioned solution was training programs, with 50% of mentions. This suggests that many companies believe that the biggest problem in cybersecurity is the lack of awareness or preparation among employees.

Close behind, collaboration frameworks made up 42.9% of responses, pointing to the idea that many organizations, especially SMEs, cannot manage cybersecurity alone and would benefit from different strategies combined (e.g., training programs, modern tools/and inputting policies).

Lastly, only 7.1% mentioned basic needs like technical tools or infrastructure, showing that companies do not see tools as the main issue. This supports the idea that even though cybersecurity is a technical topic, people and teamwork are seen as more important to improving it.

This rare case of "Basic Needs" as a solution was added after an interview with an SME worker who explained that in their particular case, they would start with better critical thinking and add solutions such as an upgrade on their ease. In other words, they recommended basic responses to a finer experience in their cybersecurity, such as limiting the trust of the computer password or not having their account logged in the company's all-use computer (M, Company Representative SMEs, 2025)[9].

Figure 6. Problem-Solution Matrix from the Interviews.

Problem-Solution Matrix General					
Hypotheses/Solutions	Training	Modern Tools	Policy changes	Collaboration	Basic Needs
Human Error	7			3	1
Outdated Technology	1				
Resource Limits				7	

Source: Own Author's elaboration from the responses extracted from the Interviews.

As with the articles, it was relevant to apply the same thinking process to the interview results, namely, how the interviewees linked each problem with a solution(s).

Therefore, human error was the most frequent issue and was mostly linked to the need for training, which was mentioned seven times. This confirms the results from the pie chart and shows that workers' behavior and mistakes are a top concern. It was also linked to collaboration, but less frequently.

On the other hand, resource limits were strongly tied to collaboration frameworks, suggesting that the best viewed solution was a mixture of more than two of the ones mentioned or more external issues, such as a combination of a need for more knowledge in the ambit of where to look for the information.

Finally, outdated technology was only mentioned once and connected to training, meaning that very few saw this as the idea that soft solutions like training and

[9] Interview code: TH.E_2_M_Company Representative SMEs_27_W_2025.

cooperation are more important in the eyes of businesses than complex solutions like buying new tech.

Let us look at the responses more specifically and separate the information between the company representatives and the Cyber Professionals. It can be concluded that the representatives linked the general cybersecurity problems equally between training (development of skills, educational talks, more information, among others) and collaboration on solutions. The human behaviour problem was only linked with training and development solutions, and the organizational issues were linked with a collaborative approach, as mentioned before.

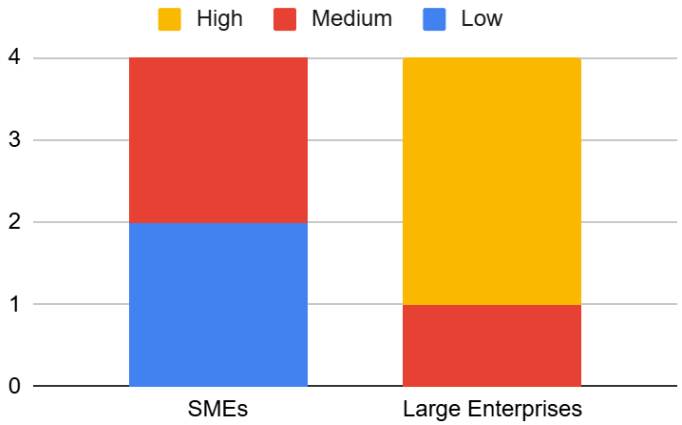
In summary, the interview results strongly support all four hypotheses, though with different emphasis depending on company size. The RBV helps explain the differences in resource access and strategy, while Organizational Culture Theory explains the role of internal practices. TAM sheds light on why SMEs may avoid adopting complex tools, and Risk Management Theory highlights the importance of structured planning, which large companies implement more often than smaller ones. The interviews show that the company's size affects how cybersecurity is managed, perceived, and planned.

2.3.2.1. Cybersecurity in SMEs and Large Companies Interviews

Although several interviewees initially held roles unrelated to cybersecurity, they began to see how their everyday actions contribute to the company's overall digital security as the conversation progressed. Many ordinary workers find it challenging to start discussing cybersecurity due to a general lack of awareness. However, when reflecting on how they handle data and manage access within the company, they acknowledge the significant impact of their practices. This shows that awareness often develops through reflection and conversation.

This growing awareness supports Hypothesis 1, which posits that large companies have a higher perception and awareness of cybercrime. According to the Organizational Culture Theory (Schein & Schein, 2017), this awareness is influenced by how well a company integrates cybersecurity into its daily practices. In larger companies, cybersecurity culture appears more institutionalized, while SMEs lack this integration.

Figure 7. Cybersecurity Awareness of the Representatives.



Source: Author's own elaboration from the information extracted from the Interviews.

SME's employees particularly mentioned that they would consider outsourcing cybersecurity if they had control over the budget. Both groups also stressed the importance of continuous training, given how fast cyber threats evolve and how difficult it can be to adapt quickly. This graph shows how opposite SMEs and larger enterprises are when discussing the level of cybersecurity awareness (considering factors such as whether they proactively incorporate these matters inside the company as part of their organizational culture).

An interesting finding is that SMEs are more likely to depend on external providers for cybersecurity. This reactive approach aligns with Risk Management Theory (Kaplan, Haimes, & Garrick, 2021).

In contrast, large companies typically have internal cybersecurity teams. This adds to the evidence that SMEs struggle with internal integration and long-term planning for cyber defense, while larger firms are more structured and proactive.

As seen, the results from the SMEs representatives show a 50% chance of the companies portraying either a low cybersecurity awareness or a medium level, referencing a process of outsourcing technical support to control cyber data and information. The grand majority of large enterprise workers (everyone but one) showed a clear high awareness in such matters, not only explaining the different training programs the company makes them go through, but even drills and simulations of cyberattacks, they were specific on how the company made them feel

responsible for their cybersecurity. These insights affirm H1 and H2, showing that larger companies' awareness and strategies are more robust.

When companies experienced an attack (often caused by human error), many adjusted their methods. They even hired additional protection or took drastic measures like dismissing an employee, yet few actually increased training efforts afterward.

Additionally, it was discovered that only one of the SMEs interviewed applied to some training program, but this was claimed as ineffective, and occurred more than three years ago, and that was the only program they remember. On the other hand, 75% of the larger companies were subjected to some extensive cybersecurity course. Nevertheless, the programs were mentioned to be repetitive and without a genuine "real-life" factor, except when specified, they were simulators of cyberattacks. A larger enterprise representative said, "It is tough to truly understand and follow the courses since there is always a voice in your head telling you, 'Oh, it will not happen! Not to me" (A, Company Representative Large, 2025)[10]. Organizational Culture Theory again becomes relevant, as cultural embedding may be as crucial as technical training.

All the companies that suffered an attack disclosed the incidents publicly, but notably, this did not lead to a drastic shift in their customer base. When asked how they would handle a cyberattack, most SMEs expressed reluctance to make a public disclosure unless necessary, resolving minor errors discreetly, to avoid harming their reputation. They were concerned that public acknowledgment might negatively affect customer trust and lead to lost business.

In contrast, large companies were more transparent. They felt that customers expect full disclosure and thorough explanations if any breach affects their data. One large company representative summed it up nicely: "I think that in the end, you create your image, and a large part of it is the trust between the two teams. It is the client's final decision." (A, Company Representative Large, 2025)[11] This contrast aligns with Risk Management Theory, which views strategic transparency as a form of damage control and reputation management.

The findings indicate that SMEs tend to treat cybersecurity as an afterthought, mainly due to cost concerns and a lack of expertise in reactive matters. They appear

[10] Interview Code: TH.E_5_A_Company Representative Large_28_W_2025.
[11] Interview Code: TH.E_5_A_Company Representative Large_28_W_2025.

to view this concern as an administration-only matter, suggesting that the issue is often handled only at the administrative level without wider integration into everyday practices.

In contrast, large companies are more likely to incorporate cybersecurity into their overall business strategy, a proactive approach, just as another interviewee mentioned. This was visual and clear when in the cases where an SME was hacked, the company representatives agreed to the slow matter control response and how that was attributed to financial loss and when in a similar situation but with a larger enterprise, because of the methods that were already ongoing the issue was able to be fixed quickly without any significant consequences.

For these organizations, cybersecurity is directly linked to protecting their reputation and ensuring compliance with external standards and regulations. This shows that cybersecurity matters and that the budget should not be viewed as a cost but as an investment. This difference in approach highlights that while SMEs often see cybersecurity as a necessary expense, larger firms view it as a strategic investment essential for long-term success.

Overall, the responses highlight the differences in how SMEs and large organizations approach cybersecurity incidents, particularly in terms of transparency, training, and risk management practice, which align not only with the theories described but also agree with the hypotheses of this work.

2.3.2.2. Cybersecurity Professionals' Interviews

A recurring theme was the significant impact of cloud technology on cybersecurity. One professional explained, "Well, especially in the cloud aspect, which is currently present. The cloud has everything on external servers," highlighting how reliance on external servers introduces new opportunities and risks.

These insights align directly with Hypothesis 4 (H4), which proposes that large companies are more likely to adopt advanced technologies. Indeed, professionals confirmed that bigger firms are not only more likely to integrate tools like cloud services and AI but also tend to have in-house teams capable of managing the risks associated with them.

Another prominent aspect discussed during the interviews was the dual nature of modern technologies. The professionals noted that when used properly, artificial

intelligence can enhance defense mechanisms and make operations safer and more effective. However, this same technology also creates vulnerabilities by potentially exposing critical information, especially when the human factor is not adequately trained to cope with the complexities.

The experts stressed that no matter how advanced the tools become, the human element remains the weakest link in cybersecurity. They put it succinctly, explaining that hackers attack the individual, not the company as a whole. This aligns with Organizational Culture Theory (Schein, 2017), which stresses that awareness and behavior are central to a secure corporate environment. Even the most advanced systems can fall short if the internal culture fails to support safe practices.

Additional insights revealed that education and resource allocation play critical roles in shaping a company's response to cyber threats (aligning with H2). Several professionals underlined the importance of combining education and resources, meaning that a successful cybersecurity strategy must combine continuous employee training with adequate financial and technological resources. This links to Risk Management Theory (Kaplan, Haimes, & Garrick, 2021).

For instance, SMEs were generally described as reactive, with cybersecurity often relegated to an administrative task rather than integrated into the company's strategic framework.

In contrast, larger organizations typically reported a proactive culture that includes regular simulations, updated training programs, and a transparent communication strategy.

One professional highlighted the significance of reputation management when dealing with cyber incidents by stating that it is a common opinion that the weight reputation and image have on a company, but the most important thing is to be transparent[12] (A, Cyber professional, 2025), reinforcing the need for openness and trust when navigating the aftermath of an attack of this nature (aligning with H3). This reinforces the Organizational Culture Theory, showing that culture and communication are as important as technical measures.

The interviews also underscored the trend towards external reliance versus internal expertise. While SMEs frequently depend on third-party providers for cybersecurity,

[12] Interview code: TH.E_10_A_Cyber professional_28_M_2025.

larger companies prefer to invest in their internal teams, sometimes even creating specialized cybersecurity departments.

The professionals agreed that, regardless of the chosen approach, the underlying challenge remains the same: ensuring every employee understands cybersecurity's critical nature. This shared understanding is crucial because, as the cyber professionals mentioned, even the most advanced technological tools will not be practical if employee practices do not align with the best security protocols. This stresses the importance of integrating a cybersecurity culture into companies.

Furthermore, the interviews revealed that professionals are aware of the pressure emerging threats, such as AI-enabled phishing scams, place on traditional and modern defense systems.

Thus, the interviews present a snapshot of current practices and serve as a call to action for continuous improvement in strategic planning and everyday operational procedures.

In summary, what the professionals shared mainly supports the four hypotheses. First, H1 is confirmed, as many have emphasized how important human behavior and cultural awareness are in preventing cyber incidents. H2 is also supported because it became clear that strategies differ greatly depending on the company size. This links directly to H3, which was reinforced by the fact that SMEs usually suffer more when attacks happen. Even though larger companies were viewed as the most targeted and the ones with a more sophisticated attack, SMEs' limited resources and reactive responses make them more vulnerable. Finally, H4 is supported since professionals mentioned that bigger firms are already adopting and managing advanced technologies like AI and cloud systems much more effectively than smaller ones.

2.3.3 Comparison between Case Studies and Interviews

Case studies from 25 academic publications offered a structured and primarily quantitative perspective. These texts focused on statistical patterns and recurring themes, highlighting measurable gaps such as limited resources, human behavior risks, and the uneven adoption of technological tools. Interviews, on the other hand, provided a more nuanced and qualitative view, capturing real-life scenarios and emotional reactions from both company representatives and cybersecurity professionals.

A key difference between the case studies and the interviews is how each defines the main cybersecurity challenge. In the case studies, the most frequent hypothesis was related to resource limitations, especially for SMEs, which connects directly with the Resource-Based View theory (Barney, 1991). However, when the interviews were conducted, participants from SMEs and large companies identified human error as the main challenge. This reveals a strong awareness among employees and a lack of proper knowledge or clear guidance on where to begin regarding cybersecurity. From a sociological perspective, this reflects a gap in cultural and educational practices within the organization, highlighted in the Organizational Culture Theory (Schein, 2017).

Another notable difference is the kind of solutions proposed. While the case studies mainly recommend policy and governance adjustments (34.2%), the interviews emphasize training and development programs, especially for SMEs. For larger companies, the solution mentioned was the combination of several approaches, showing a more cyclical and proactive internal culture, as described in the Risk Management Theory. Even though training is not the most common solution in the case studies, it still appears as the second most frequent, which means that both sources agree that the starting point is internal education.

Looking at the hypotheses/solution matrix, case studies tend to associate resource limitations with policy/governance changes, a connection that interviewees did not directly make. Instead, the interviewees saw the solution as a mix of several strategies. However, if this mix is interpreted from another angle, their idea of combining approaches could resemble collaboration frameworks, which can also reflect internal policy adjustments. Lastly, there is a clear consensus across both data types: regarding human error, training and awareness programs are the solution. This outcome reinforces the importance of organizational education and employee behavior, which are key elements in managerial planning and sociological understanding of workplace risk.

A SWOT analysis was conducted separately for each source to visualize the insights gathered[13].

The case studies consistently emphasized company size as a decisive variable, confirming that larger firms typically have better infrastructure and proactive

[13] Please find it attached in the Appendix.

strategies. Meanwhile, interviews added context about cultural, psychological, and operational challenges in everyday cybersecurity practices.

Both sources agree that human error and lack of awareness are the most critical cybersecurity threats. This convergence validates Hypothesis 1 (H1) and supports theories like the Resource-Based View, Organizational Culture Theory, and Risk Management Theory.

However, differences emerge in how theory and practice address risk. The academic literature proposes solutions on a broader policy or strategic level, whereas interviews show how personal behavior and internal dynamics influence success or failure. Both perspectives present a fuller picture (quantitative structure meets qualitative depth), demonstrating that effective cybersecurity requires systems and stories.

2.3.4 Practical Implications

First and foremost, businesses need to integrate cybersecurity into the core of their strategic planning. Relying solely on technical fixes or sporadic training programs is not enough; rather, an approach that considers culture, technology, and human behavior is crucial.

The findings suggest that even with limited resources, basic yet effective measures can significantly improve SMEs' security posture. The interviews reveal that SMEs often adopt a reactive posture; this perspective needs to shift toward a proactive stance where even low-cost measures, such as robust password policies, periodic basic training sessions, and implementing simple access control protocols, can significantly enhance their security posture. Additionally, SMEs may benefit from outsourcing technical tasks to specialized providers if these external teams are integrated into a broader, internally driven cybersecurity culture.

Large companies, on the other hand, while generally more resource-rich, face their own set of challenges. The data shows that these organizations tend to have a more established cybersecurity culture and a greater capacity to invest in advanced technologies. However, the interviews indicate that even in these settings, the continuous evolution of cyber threats needs ongoing adaptation. Regular simulations, updated training modules that include "real-life" scenarios, and maintaining a high degree of transparency with clients and stakeholders are

highlighted as critical practices, which encapsulate the strategic importance of trust and transparency.

The practical implications extend to how companies manage crisis communication and post-incident analysis. Case studies and interviews stress that while a cyberattack's immediate financial and operational impacts can be severe, the long-term damage to reputation is perhaps the most critical. In this regard, cultivating a culture of transparency can mitigate reputational harm, as it reassures customers that the organization is committed to accountability and continuous improvement.

The findings from the interviews and literature review yield additional practical implications for business practice and policy. For example, tailored cybersecurity strategies are needed: SMEs require cost-effective, scalable solutions tailored to their specific vulnerabilities, while large enterprises should focus on integrating advanced technologies with robust internal controls.

Most SME interviewees admitted that their companies outsource cybersecurity without the financial control or staff knowledge to manage it in-house. However, the case studies suggest that these limitations can be partly solved with governance improvements and better policy design, something that SMEs in the interviews did not mention directly. This means that more awareness is needed about technology, organizational design, and strategic planning. Business managers should view cybersecurity as an investment, not a cost. They must be encouraged to allocate resources with a long-term strategy in mind, even if that strategy starts small.

Policy recommendations from this study suggest that policymakers should consider creating incentives for SMEs to adopt advanced cybersecurity measures. This might include subsidies for cyber insurance, tax benefits for investments in cybersecurity training, or other support mechanisms that help smaller companies overcome resource constraints. Furthermore, controlling access to data with a well-defined access management plan should be integral to any cybersecurity risk management policy. An effective access management plan should establish clear guidelines about when and how employees can access critical information and networks.

Finally, this study shows how different levels of hierarchy and professional fields perceive the same threat differently. For example, company representatives often focused more on budget issues, while cybersecurity professionals emphasized threats' technical complexity and fast-changing nature. This disconnect can create delays in decision-making or missed opportunities for improvement. Managers

should consider bridging this gap by involving technical staff and general employees in decision-making, making cybersecurity a shared responsibility rather than a specialized task.

Overall, the practical implications derived from this research urge SMEs and large companies to consider cybersecurity not simply as a set of isolated technical measures but as an integral part of overall business strategy. This means aligning budgetary decisions, staff training, leadership commitment, and communication protocols with the goal of risk mitigation and operational resilience. The interviews and literature review findings offer a set of best practices that include tailored cybersecurity strategies, investment in human capital, cross-departmental collaboration, and supportive policy recommendations, all of which contribute to a stronger and more resilient digital future.

Chapter 3. Conclusion

This research explored how small and medium-sized enterprises (SMEs) and larger corporations in Catalonia perceive, experience, and manage the rising threat of cybercrime. Drawing from a systematic analysis of 25 case-based publications and 12 semi-structured interviews with company representatives and cybersecurity professionals, this thesis aimed to bridge the gap between theoretical and on-the-ground organizational realities. Anchored in the Resource-Based View (RBV) and Organizational Culture Theory, and complemented by the Technology Acceptance Model (TAM) and Risk Management Theory, this study provides a managerial lens to evaluate how cyber risk is perceived and addressed across business contexts.

The study proposed four main hypotheses, each addressing different dynamics of cybersecurity management: perception, strategy implementation, impact, and adoption of technology. The findings largely support these hypotheses.

Table 4. Confirmed Hypotheses.

HYPOTHESIS	CONFIRMED/DENIED	PROOF
H1: Larger companies have higher awareness of cybercrime than SMEs	Confirmed	SMEs treated cybersecurity as secondary. Larger enterprises treated it from a strategic priority. (Organizational Culture Theory)
H2: Larger companies implement more comprehensive cybersecurity strategies	Confirmed	Large firms: proactive. SMEs: reactive. (Resource-Based View)
H3: SMEs experience more severe impacts from cyberattacks	Partially Confirmed	SMEs faced prolonged operational disruptions when hacked, large firms recovered faster (Risk Management Theory)
H4: Large firms are more likely to adopt advanced cybersecurity technologies	Confirmed	Large firms integrated AI/Cloud tools; SMEs mentioned cost/complexity barriers (TAM)

Source: Own Author's elaboration.

As described above, the first hypothesis was confirmed through the literature and interview data, which show that larger companies demonstrate higher awareness levels due to their greater resources and exposure. SMEs acknowledge the risks but often express uncertainty about where or how to begin, revealing a gap in structured awareness mechanisms.

The case studies also revealed that structured policy frameworks and risk governance models are more common among large firms. Interview data echoed this, especially through the proactive integration of cybersecurity into organizational decision-making. SMEs, in contrast, tend to rely on more reactive and fragmented approaches, often constrained by budget and expertise.

The third hypothesis was partially confirmed because SMEs are more vulnerable due to limited resources, but some large enterprises also reported severe consequences,

especially reputational damage. However, when attacks occurred, SMEs demonstrated higher operational fragility, aligning with the RBV's emphasis on internal capacities.

Lastly, adopting artificial intelligence tools, cloud security measures, and continuous monitoring systems is more prevalent in large companies. However, a few SMEs were willing to adopt such tools if guidance and cost-effective solutions were available, showing a desire to bridge the technological divide.

Both data sets reveal that human error remains one of the most cited internal vulnerabilities, reaffirming the need for internal education and cultural alignment around cybersecurity norms. The Organizational Culture Theory proved particularly useful in interpreting how awareness, leadership, and interdepartmental collaboration can shape the effectiveness of cyber strategies.

From a managerial perspective, strategic resource allocation emerged as a determining factor in building cybersecurity resilience. The contrast between SMEs and large corporations regarding risk assessment formality and preparedness is not merely a matter of budget but leadership prioritization. Interestingly, many interviewees emphasized the need for multi-solution frameworks over singular tools, especially in larger corporations, pointing to a cultural maturity and cyclical proactivity not always present in SMEs.

A key practical implication is the consistent alignment between case studies and interviews in identifying training and internal awareness as the most immediate, scalable, and effective solution to mitigating human error. Moreover, the gap observed in SMEs regarding policy and governance structures suggests an urgent need for public-private collaboration to design tailored support mechanisms.

This thesis also contributes methodologically by combining qualitative interview data with AI-supported article analysis to build a dual-layered understanding. Although not a systematic review per se, the study offers a structured thematic synthesis capable of informing future work in cybersecurity management.

In conclusion, cybersecurity is not solely a technical matter but a deeply embedded organizational and social issue. The findings validate the research objectives, confirm the theoretical underpinnings of the study, and demonstrate the necessity for integrated, culture-driven, and size-sensitive approaches to managing cyber risk in

contemporary enterprises. As digital threats evolve, so must our understanding (and management) of them.

3.1 Limitations and Future Research

While this study provides valuable insights into the cybersecurity challenges faced by SMEs and large enterprises in Catalonia, several limitations should be acknowledged:

The study is based on interviews with eight companies and four cybersecurity professionals. Although the findings offer a useful snapshot, a larger sample could provide more generalizable results.

Focusing exclusively on Catalonian enterprises limits the results' applicability to other regions. Future research could expand the geographic scope to compare different regional approaches to cybersecurity.

Cybersecurity is a rapidly evolving field. The study's findings are based on current practices and perceptions; however, the continuous advancement in cyberattack techniques may require ongoing research to keep pace with emerging trends.

While combining a standard literature review and interviews offers a comprehensive view, future studies might benefit from mixed-method approaches that include quantitative measures to validate the findings further.

Future research directions should focus on expanding the sample size to include a broader range of industries and regions, investigating the effectiveness of specific cybersecurity interventions and training programs, and exploring the role of emerging technologies in enhancing and undermining cybersecurity defenses.

In summary, this thesis has highlighted key differences and commonalities in the cybersecurity strategies of SMEs and large enterprises. It has underscored the critical role of organizational culture and human resource practices in mitigating cyber risks. Despite its limitations, the study offers practical implications and a foundation for future research in this essential field.

References

Adriko, R., & Nurse, J. R. C. (2024). Cybersecurity, cyber insurance and small-to-medium-sized enterprises: A systematic review. Information and Computer Security, 32(5), 691–710. https://doi.org/10.1108/ICS-01-2024-0025

Al-Somali, S. A., Saqr, R. R., Asiri, A. M., & Al-Somali, N. A. (2024). Organizational Cybersecurity Systems and Sustainable Business Performance of Small and Medium Enterprises (SMEs) in Saudi Arabia... Sustainability, 16(5), 1880. https://doi.org/10.3390/su16051880

Alahmari Ph.D., Abdulmajeed & Duncan, Bob. (2020). Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. 1–5. 10.1109/CyberSA49311.2020.9139638

Amrin, N. (2014). The impact of cyber security on SMEs [Master's thesis, University of Twente]. University of Twente Student Theses. https://purl.utwente.nl/essays/65851

Ansbach, J., & Sharton, B. (2020). Preventing insider threats to cybersecurity. Risk Management, 67(8), 12–13. https://www.proquest.com/magazines/preventing-insider-threats-cybersecurity/docview/2479813664/se-2

Aschwanden, R., Messner, C., Höchli, B., & Holenweger, G. (2024). Employee behavior: the psychological gateway for cyberattacks. Organizational Cybersecurity Journal, 4(1), 32–50. https://doi.org/10.1108/OCJ-02-2023-0004

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Information and Computer Security, 27(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Barney, J. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17(1), 99–120. https://doi.org/10.1177/014920639101700108

Buehrly-Harris, L. (2024). Applying Predictive Behavioral Theories to Phishing Email Defense... ProQuest Dissertations & Theses.

https://www.proquest.com/dissertations-theses/applying-predictive-behavioral-theories-phishing/docview/3042949880/se-2

Chang, F. R. (2012). Guest editor's column. The Next Wave, 19(4), 1–2. https://www.nsa.gov/Portals/70/documents/resources/everyone/digital-media-center/publications/the-next-wave/TNW-19-4.pdf

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cybersecurity of small-to-medium businesses: Challenges, research focus, and recommendations. IEEE Access, 10, 85701–85719. http://dx.doi.org/10.1109/ACCESS.2022.3197899

Corradini, I. (2020). Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology. Springer International Publishing. https://doi.org/10.1007/978-3-030-43999-6

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review, 4(10), 13–21. https://doi.org/10.22215/timreview835

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008

DiMaggio, P. J., Powell, W. W., Dobbin, F., & Baum, J. A. C. (2000). The iron cage revisited institutional isomorphism and collective rationality in organizational fields. In Economics Meets Sociology in Strategic Management (Vol. 17, pp. 143–166). Emerald Group Publishing Limited. https://doi.org/10.1016/S0742-3322(00)17011-1

Dirksen, J. (2022). Helping cybersecurity teams solve risk, HR & compliance issues. BenefitsPRO. https://www.proquest.com/trade-journals/helping-cybersecurity-teams-solve-risk-hr-amp/docview/2688239916/se-2?accountid=14733

Epstein, A. J. (2023). Thinking strategically about cyber risk. Business Horizons, 66(3), 341–355. https://www.proquest.com/trade-journals/thinking-strategically-about-cyber-risk/docview/1634874008/se-2?accountid=14733

European Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. (2003). Official Journal of the European Union, L 124, 36–41.

Fisher, R., Porod, C., & Peterson, S. (2021). Motivating Employees and Organizations to Adopt a Cybersecurity-Focused Culture. Journal of Organizational Psychology, 21(1), 114–131. https://doi.org/10.33423/jop.v21i1.4030

Funcas. (2024, June 27). Las pymes españolas generan seis de cada diez puestos de trabajo en el sector empresarial. Retrieved May 13, 2025, from https://www.funcas.es/prensa/las-pymes-espanolas-generan-seis-de-cada-diez-puestos-de-trabajo-en-el-sector-empresarial/

International Organization for Standardization. (2013). ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems . Requirements. https://www.iso.org/standard/54534.html

Kaplan, S., Haimes, Y. Y., & Garrick, B. J. (2001). Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinement to the Quantitative Definition of Risk. Risk Analysis, 21(5), 807–807. https://doi.org/10.1111/0272-4332.215153

Ley 14/2013, de 27 de septiembre, de apoyo a los emprendedores y su internacionalización. (2013). Boletín Oficial del Estado, 233, 78787–78882.

Manky, D. (2013). Cybercrime as a service: a very modern business. Computer Fraud & Security, 2013(6), 9–13. https://doi.org/10.1016/S1361-3723(13)70053-8

Mhlongo, T., van der Poll, J. A., & Sethibe, T. (2023). A Control Framework for a Secure Internet of Things within Small-, Medium-, and Micro-Sized Enterprises in a Developing Economy. Computers (Basel), 12(7), 127-. https://doi.org/10.3390/computers12070127

Murphey, D. (2020). How your HR department can help to overcome the cybersecurity skills gap. BenefitsPRO. https://www.proquest.com/trade-journals/how-your-hr-department-can-help-overcome/docview/2376391277/se-2?accountid=14733

Osawaru, G. (2024). Electronic Health Record Data Breaches in U.S. Healthcare Industry: A Quantitative Study Using the Protection Motivation Theory (PMT) to Mitigate Data Breaches. ProQuest Dissertations & Theses. https://www.proquest.com/publiccontent/dissertations-theses/electronic-health-record-data-breaches-u-s/docview/3058334093/sem-2?accountid=14733

Paulsen, C. (2016). Cybersecuring Small Businesses. Computer (Long Beach, Calif.), 49(8), 92–97. https://doi.org/10.1109/MC.2016.223

Przybyszewski, K., Małagocka, K., & Przymus, Z. (2024). Identifying cyberrisk factors in hybrid workforce environments. Scientific Papers of Silesian University of Technology, (184), 1437–1445. https://doi.org/10.29119/1641-3466.2023.184.20

Przymus, P., Alhazmi, A. A., & Gough, O. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. Technological Forecasting and Social Change, 202, 123115. https://doi.org/10.1016/j.techsoc.2024.102670

PwC. (2020). Fighting fraud: A never-ending battle – PwC's Global Economic Crime and Fraud Survey 2020. https://www.pwc.be/en/FY20/documents/global-economic-crime-fraud-survey-2020.pd

PwC. (2025). Bridging the gaps to cyber resilience: The C-suite playbook – Findings from the 2025 Global Digital Trust Insights. https://www.pwc.es/es/publicaciones/consultoria/global-digital-trust-insights-2025.pdf

Rawindaran, N., Jayal, A., & Prakash, E. (2022). Exploration of the Impact of Cybersecurity Awareness on Small and Medium Enterprises (SMEs) in Wales Using Intelligent Software to Combat Cybercrime. Computers, 11(12), 174. https://doi.org/10.3390/computers11120174

Rawindaran, N., Nawaf, L., Alarifi, S., Alghazzawi, D., Carroll, F., Katib, I., & Hewage, C. (2023). Enhancing Cyber Security Governance and Policy for SMEs in Industry 5.0: A Comparative Study between Saudi Arabia and the United Kingdom. Digital, 3(3), 200–231. https://doi.org/10.3390/digital3030014

Reglamento general de protección de datos (RGPD) | EUR-Lex - Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

Roberts, S. A. (2021). Exploring the Relationships Between User Cybersecurity Knowledge, Cybersecurity and Cybercrime Attitudes, and Online Risky Behaviors. ProQuest Dissertations & Theses. https://www.proquest.com/publiccontent/dissertations-theses/exploring-relationships-between-user/docview/2506630550/sem-2?accountid=14733

Santos, O. (2024). Developing cybersecurity programs and policies in an AI-driven world (4th ed.). Pearson.

Schein, E. H., & Schein, P. (2017). Organizational culture and leadership (5th edition). John Wiley and Sons, Inc.

Singer, P. W., & Pratt, S. (2016). Cybersecurity and Cyberwar [Broadcast]. Tantor Media, Inc.

Singh, M. M., & Bakar, A. A. (2019). A Systemic Cybercrime Stakeholders Architectural Model. Procedia Computer Science, 161, 1147–1155. https://doi.org/10.1016/j.procs.2019.11.227

Stanton, M., Ernst, G., & Janik, A. L. (2017). Cybersecurity best practices. Computer and Internet Lawyer, 34(4), 22-25. https://www.proquest.com/trade-journals/cybersecurity-best-practices/docview/1881688407/se-2?accountid=14733

Triplett, W. J. (2022). Addressing Cybersecurity Leadership Challenges in Organizations. ProQuest Dissertations & Theses. https://www.proquest.com/publiccontent/dissertations-theses/addressing-cybersecurity-leadership-challenges/docview/2816676527/sem-2?accountid=14733

Via Empresa. (2023, July 11). Las 14 pymes catalanas que están cambiando el mundo (D. Lombrana, Ed.). Retrieved January 2, 2025 from https://www.viaempresa.cat/es/empresa/14-pymes-catalanas_2185301_102.html

VIJAYAKUMAR, U., & ILANGOVAN, D. (2015). A Quantitative Approach to Information Systems Audit in Small and Medium Enterprises. Informatica Economica, 19(3/2015), 89–95. https://doi.org/10.12948/issn14531305/19.3.2015.08

Watad, M., Washah, S., & Perez, C. (2018). IT security threats and challenges for small firms: Managers' perceptions. International Journal of the Academic Business World, 12(1), 23–30.

World Bank. (2019, October 16). Small and Medium Enterprises (SMEs) Finance. Retrieved May 10, 2025, from https://www.worldbank.org/en/topic/smefinance

Zielinski, D. (2019). 5 Top Cybersecurity Concerns for HR in 2019. HRNews. https://www.proquest.com/trade-journals/5-top-cybersecurity-concerns-hr-2019/docview/2188219411/se-2?accountid=14733