Leveraging Cybersecurity Maturity for Competitive Advantage

A Model for SMEs

M.J.H. Gringhuis

First supervisor:
Dr. A. Abhishta

Second supervisor:
Dr. M. de Visser

Master of Business Administration
University of Twente
March 18, 2025

Abstract

Small and medium-sized enterprises (SMEs) often perceive cybersecurity as purely a defensive necessity, yet this research challenges that view by highlighting its strategic value. This study explores the direct relationship between Cybersecurity Maturity and Competitive Advantage in SMEs, filling a significant gap in the existing literature where quantitative proof is absent. While much of the existing research focuses on large corporations, this study offers empirical evidence of how cybersecurity maturity can serve as a powerful competitive differentiator for SMEs.

The study employs a quantitative, non-experimental correlational design, analysing key constructs such as Cybersecurity Maturity, Competitive Advantage, regulatory compliance, and the frequency of cyber incidents. Data was collected through a cross-sectional self-assessment survey targeting SMEs, and the analysis was conducted using Partial Least Squares Structural Equation Modeling (PLS-SEM) with ADANCO.

The results of this study reveal a statistically significant direct effect of Cybersecurity Maturity on Competitive Advantage. SMEs with higher levels of Cybersecurity Maturity experience enhanced customer trust, operational resilience, and market differentiation factors contributing to long-term success. This supports the concept that cybersecurity investments should be viewed as a strategic asset, enabling SMEs to gain a Competitive Advantage.

The study also examined regulatory compliance and the frequency of cyber incidents as potential mediators in the relationship between Cybersecurity Maturity and Competitive Advantage. These mediating effects were not statistically significant, suggesting that while regulatory compliance and reduced cyber incidents are important for operational stability, they do not mediate the effect of Cybersecurity Maturity on Competitive Advantage.

This study shifts the conversation around cybersecurity from being a cost to adding value. It demonstrates that SMEs prioritizing Cybersecurity Maturity do not just protect their businesses; they can use it to gain a sustainable Competitive Advantage. By presenting quantitative evidence of cybersecurity's role in Competitive Advantage, this research provides SMEs with a compelling business case to invest in cybersecurity as a driver of growth and differentiation. While recognizing its limitations, this study lays the groundwork for future research to explore further how Cybersecurity Maturity can shape SME success in an increasingly digital economy.

Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Definition
CCAM	Cybersecurity Capability Assessment Model
CLT	Central Limit Theorem
CT	Consumer Trust
DFC	Differentiation from Competition
ENISA	European Union Agency for Cybersecurity
FCI	Frequency of Cyber Incidents
GDPR	General Data Protection Regulation
NIS2	Network and Information Systems 2
ORC	Operational Resilience and Continuity
PEO	People
PLS-SEM	Partial Least Squares Structural Equation Modeling
PPT	People-Process-Technology
PRO	Process
RC	Regulatory Compliance
SME	Small and Medium-sized Enterprises
SRMR	Standardized Root Mean Square Residual
TEC	Technology
d_{ULS}	Squared Euclidean Distance
VIF	Variance Inflation Factor

1 Introduction

Many managers in small and medium-sized enterprises (SMEs) struggle to secure sufficient funding to enhance their Cybersecurity Maturity (Junior et al., 2023). While the risks posed by cyber threats are well-documented, decision-makers in SMEs often struggle to allocate resources to cybersecurity due to limited budgets, competing priorities, and the perception that cybersecurity investments yield limited financial returns.

Although financial constraints may limit cybersecurity investment, overlooking it can be a missed opportunity. Cybersecurity Maturity can offer SMEs more than just protection; it can serve as a driver of Competitive Advantage. This research explores how SMEs can leverage Cybersecurity Maturity to gain a Competitive Advantage. To provide empirical insights, this study employs a quantitative approach to examine the relationship between Cybersecurity Maturity and Competitive Advantage in SMEs. It will help SMEs understand that cybersecurity is not just a defensive measure but also an opportunity to differentiate themselves in the marketplace. By adopting this perspective, SMEs can see cybersecurity as a strategic investment that protects operations, builds customer trust, enhances resilience, and fosters long-term competitiveness. (Lloyd, 2020).

While cybersecurity can provide individual SMEs with a competitive edge, its impact extends far beyond the firm level. Cybersecurity breaches affect entire industries, economies, and public trust in digital systems (Saravanan & Babu, 2024). In recent years, the growing prevalence of cyberattacks has highlighted the vulnerabilities that enterprises face (Admass et al., 2024). From data breaches to ransomware attacks, the consequences of cyber incidents can be devastating (e.g., going out of business). Cybersecurity is needed for people to maintain trust in digital systems, ensure personal data privacy, and safeguard the integrity of online activities. Without strong cybersecurity measures in place, businesses and customers alike are exposed to increasing risks.

As these cyber threats evolve, companies must ensure that their products and services are secure to maintain customer confidence and remain competitive in the marketplace (Mmango & Gundu, 2024). Ensuring product and service security is particularly crucial for SMEs, which often lack the resources to implement advanced cybersecurity measures. Despite their smaller size, SMEs face significant cybersecurity threats that can lead to financial and reputational damage (ENISA, 2021).

However, unlike larger organizations with dedicated cybersecurity departments, many SMEs may be unaware of cybersecurity's importance or believe they are not attractive targets for cybercriminals (Wilson et al., 2023). In fact, SMEs are increasingly being targeted, and the cost of cyber incidents can be devastating to their operations (EU, 2022).

Furthermore, SMEs often face significant barriers to adopting new practices or technologies due to limited financial, technical, and human resources (Van Burg et al., 2012). These constraints make incentives critical for driving change and fostering innovation within the SME sector.

Incentives, such as tax benefits, grants, and subsidies, can help mitigate the perceived risks and costs associated with implementing improvements in sustainability, technology adoption, and cybersecurity (Barney, 1991; Lee & Peterson, 2000). Additionally, governments and industry bodies play a vital role in creating frameworks that encourage SMEs to comply with new standards and adopt practices that enhance their competitiveness (Gibb, 2000).

As incentives help SMEs overcome financial and technical barriers, cybersecurity can shift from being a burden to a Competitive Advantage in several ways. First, robust cybersecurity measures can enhance a company's reputation and build trust with their customers and stakeholders, who are increasingly concerned about their data privacy and security (Rohan et al., 2022). SMEs that demonstrate their commitment to protecting their customers' data are more likely to attract and retain their customers, thereby gaining a competitive edge (Hassan & Ahmed, 2023). Second, effective cybersecurity practices can prevent costly data breaches and cyberattacks, which can have severe financial and operational consequences for SMEs that have limited resources (Arroyabe, 2023). Proactively addressing cybersecurity helps SMEs avoid potential downtime and economic losses due to cyber incidents. Furthermore, as governing agencies continuously tighten data protection regulations, SMEs prioritizing cybersecurity will be better positioned to comply with evolving regulations, avoid penalties, and strengthen their market position (Henson & Sutcliffe, 2017).

Cybersecurity can serve as a powerful enabler of growth and innovation (Barbier et al., 2016). Organizations leveraging their Cybersecurity Maturity as a Competitive Advantage can accelerate their innovation processes and bring new products or services to market more efficiently (Lloyd, 2020). Conversely, a lack of robust cybersecurity measures can halt innovation, as concerns over potential vulnerabilities or breaches may delay or even terminate the development of new initiatives (Barbier et al., 2016).

While extensive research has explored how SMEs can enhance their cybersecurity practices and reduce the associated risks, limited attention has been given to its strategic benefits, particularly in the context of Competitive Advantage (Mmango & Gundu, 2024). Existing studies mainly focus on risk mitigation and protection, overlooking how Cybersecurity Maturity can contribute to consumer trust, differentiation, and resilience, which are all key drivers of competitiveness in SMEs. This study aims to fill this gap by examining how Cybersecurity Maturity contributes to Competitive Advantage in SMEs, with regulatory compliance and the frequency of cyber incidents serving as mediators. By exploring how cybersecurity can transform from a financial burden into a strategic asset, this research seeks to provide valuable insights into how SMEs can leverage cybersecurity to gain a Competitive Advantage.

To empirically examine these relationships, this study adopts a quantitative research design, employing a survey-based approach to collect data from SMEs. The analysis will be conducted using partial least squares structural equation modeling (PLS-SEM) to examine the relationship between Cybersecurity Maturity and Competitive Advantage. This methodology will also allow the identification of mediating factors, such as regulatory compliance and the frequency of cyber incidents, shedding light on how Cybersecurity Maturity can translate into a competitive edge

for SMEs.

1.1 Aim of the Study

This study investigates how SMEs can leverage Cybersecurity Maturity to gain a Competitive Advantage. While cybersecurity is often viewed merely as a defensive measure to mitigate risks, this study will explore its potential as a strategic asset to enhance Competitive Advantage. The central research question guiding this study is:

To what extent can small and medium-sized enterprises (SMEs) gain Competitive Advantage through Cybersecurity Maturity?

To answer this question, the study examines the following sub-questions:

- **How is Cybersecurity Maturity defined and assessed in the context of SMEs?**
  - To answer this sub-question, a thorough review of existing literature will be conducted. Various definitions and theoretical frameworks for Cybersecurity Maturity will be analysed, focusing on their relevance to SMEs. This analysis will help identify key dimensions and assessment methods tailored to SMEs' unique challenges and resource constraints.

- **What are the key dimensions of Competitive Advantage, and how can these be assessed?**
  - This sub-question will be answered by reviewing the literature to identify widely accepted dimensions of Competitive Advantage. Additionally, metrics and tools for assessing these dimensions in the context of SMEs will be explored. Theoretical frameworks will be compared and evaluated to ensure the analysis aligns with the unique characteristics and competitive dynamics of SMEs.

- **What other factors affect the relationship between Cybersecurity Maturity and Competitive Advantage?**
  - To address this sub-question, a comprehensive literature review will be conducted to identify potential moderating and mediating factors that influence the relationship between Cybersecurity Maturity and Competitive Advantage. The review will examine academic studies, industry reports, and theoretical frameworks to explore various variables. These insights will provide a theoretical foundation for understanding the complex interplay of factors that shape this relationship in the SME context.

- **How can the relationship between Cybersecurity Maturity and Competitive Advantage in SMEs be explained based on empirical findings?**
  - An empirical study will be conducted using PLS-SEM to address this sub-question. Data collected from SMEs will be analysed to examine the relationships between Cybersecurity Maturity, Competitive Advantage, and potential mediating factors. The results of the analysis, including path coefficients, significance levels, and explained variance (R^2), provide insights into the strength and direction of these relationships. By interpreting these

findings, this study aims to validate theoretical assumptions and offer empirical evidence on how Cybersecurity Maturity contributes to Competitive Advantage in SMEs.

1.2 Paper Outline

The remainder of this paper will follow the subsequent structure. Chapter 2 reviews the existing literature on the foundational constructs relevant to the relationship between Cybersecurity Maturity and Competitive Advantage. Furthermore, the hypotheses and conceptual model are presented. Chapter 3 outlines the methodology used to test the hypotheses and conceptual model. Chapter 4 presents the results of the applied methods and analyses the data. Chapter 5 discusses the key findings of the study, their interpretations, and the broader research implications. The study's limitations are acknowledged, and recommendations for future research are provided. Chapter 6 presents the conclusions drawn from this research.

2 Theoretical Background

This section outlines the theoretical foundation for understanding the relationship between Cybersecurity Maturity and Competitive Advantage in SMEs. It begins by discussing the growing importance of cybersecurity in SMEs, emphasizing their vulnerability to cyber threats and the need for effective cybersecurity practices. The section then introduces key constructs, including Cybersecurity Maturity, Competitive Advantage, regulatory compliance, and the frequency of cyber incidents.

The constructs are analysed in the context of the People-Process-Technology (PPT) framework for Cybersecurity Maturity, and Competitive Advantage is explored through trust, differentiation, and resilience (Handri et al., 2023). The relationships between these constructs are examined, focusing on how Cybersecurity Maturity influences Competitive Advantage, mediated by regulatory compliance and the frequency of cyber incidents. The section concludes with a conceptual model that integrates these ideas, highlighting the pathways through which Cybersecurity Maturity could enhance SMEs' competitive positioning.

2.1 The Evolution of Cybersecurity Research in SMEs

The increasing reliance of businesses on digital technologies has driven a significant surge in cybersecurity research (Algan, 2019). A bibliometric analysis of the literature on cybersecurity in SMEs by Truong and Nguyen (2024) reveals a steady growth in scholarly interest. This trend underscores the escalating recognition of SMEs as both critical contributors to economies and vulnerable targets for cyber threats.

The majority of the research focuses on how SMEs can improve their Cybersecurity Maturity (Truong & Nguyen, 2024). Key focus areas of the research include employee training, which aims to reduce human error vulnerabilities; the implementation of risk assessment frameworks to identify and mitigate potential threats; and technological investments such as firewalls and intrusion detection systems to improve security infrastructure (El-Hajj & Mirza, 2024; Lucas & Harlee, 2024; Weston & Faisal, 2024). These studies provide valuable insights into practical measures SMEs can adopt to enhance their cybersecurity.

However, research has shown that SME owners are still prone to underestimate the cybersecurity risk that they are susceptible to (Wilson et al., 2023). A survey on SMEs in the United States showed that half of the studied SMEs had not invested in cybersecurity because they thought they did not store any valuable data when they did store social security numbers and credit card details of clients (Chidukwani et al., 2022). This underestimation of cyber risk leaves SMEs vulnerable to potential attacks that could have severe consequences. Without proper cybersecurity measures, SMEs are at risk of financial loss, reputational damage, and operational disruptions (Alharbi et al., 2021). Even SMEs that have implemented cybersecurity practices and strategies tend to become complacent in maintaining them due to the lack of visible benefits from the effort and expense (Chidukwani et al., 2022).

This lack of awareness and perceived absence of immediate benefits highlight a critical barrier to improving Cybersecurity Maturity among SMEs. Without a clear understanding of why cybersecurity matters, not only as a defensive measure but also as a strategic enabler, SMEs are less motivated to invest in and sustain robust cybersecurity practices (Wilson et al., 2023). Current research predominantly focuses on how SMEs can enhance cybersecurity but offers limited insight into why they should prioritize these improvements, particularly in terms of potential Competitive Advantages. Bridging this gap in understanding is crucial for motivating SMEs to adopt a proactive stance toward cybersecurity.

Little research has been done into how Cybersecurity Maturity could lead to Competitive Advantage for SMEs. Frameworks such as the Cybersecurity Capability Assessment Model (CCAM) developed by Kosutic (2021), address how Cybersecurity Maturity can lead to Competitive Advantage but are not specifically tailored to SMEs. Mmango and Gundu (2024) state in their systematic literature review that there is a need for adaptive cybersecurity frameworks that link cybersecurity to Competitive Advantage and also fit SMEs.

Given these gaps in the literature, this research adopts a quantitative approach to investigate the role of cybersecurity in driving Competitive Advantage for SMEs. By focusing specifically on SMEs, this study aims to explore how Cybersecurity Maturity can enhance their Competitive Advantage by improving trust, resilience, and differentiation from the competition. This approach aligns with recent calls for research addressing SMEs' unique cybersecurity needs and investigates how these practices can be leveraged strategically to strengthen their competitive positions (Mmango & Gundu, 2024).

2.2 Foundational Constructs in Cybersecurity and Competitive Advantage

To be able to effectively investigate the role of cybersecurity in driving Competitive Advantage for SMEs, it is essential to first understand the foundational constructs that form the basis of this relationship. By exploring the dimensions of Cybersecurity Maturity and Competitive Advantage, this section helps to understand how these constructs interact and contribute to the strategic positioning of SMEs in the digital landscape.

2.2.1 Cybersecurity Maturity

Cybersecurity Maturity is the degree to which an organization has developed and implemented robust cybersecurity practices and is ready to defend itself and its digital assets against cyberattacks. In the context of this research, Cybersecurity Maturity is explored through the lens of the People-Process-Technology (PPT) framework, which is a foundational model for understanding and improving organizational capabilities (Handri et al., 2023).

The Role of People

The "people" aspect of cybersecurity refers to the role of humans in safeguarding an organization against cyber threats. Skilled and knowledgeable employees are essential for identifying,

mitigating, and responding to cybersecurity challenges.

For organizations to develop a robust cybersecurity posture, employees should be well-informed and vigilant about cybersecurity best practices. This includes having the ability to recognize phishing attempts, handle sensitive data securely, and adhere to organizational security protocols. Regular and targeted training programs are essential in fostering a culture of security awareness across all levels of the organization (Hwang et al., 2021).

A key component of this culture is the clear definition of roles and responsibilities within the organization. Accountability is vital for maintaining a cohesive and effective cybersecurity strategy. Designated roles, such as cybersecurity specialists, IT personnel, and managerial staff, must work collaboratively to align cybersecurity initiatives with broader organizational objectives. This structured approach ensures coordinated responses to cyber threats and minimizes operational inefficiencies, enhancing the organization's overall resilience (Alshaikh, 2020). While a skilled workforce forms the foundation, structured processes are essential to guide actions and ensure preparedness.

The Role of Process

The "process" dimension of cybersecurity focuses on the structured practices and procedures that enable organizations to manage cybersecurity incidents and prepare for incidents. Effective processes help organizations not only be reactive but also proactive in assessing, mitigating, and recovering from cyber threats.

The development and regular testing of response and recovery plans are fundamental for organizational cyber resilience (Halikias, 2024). Testing these plans helps personnel understand their roles during a cyber incident, reducing confusion and wasting of time in critical moments. The testing also helps identify gaps or inefficiencies in the plans, allowing the organization to improve them.

Another critical aspect of cybersecurity processes is the integration of risk assessment when selecting partners (Keskin et al., 2021). Organizations can build a more secure and resilient network by implementing standardized risk management practices and maintaining clear communication with supply chain partners.

The Role of Technology

In the PPT model, the "technology" dimension represents the tools and systems organizations can use to safeguard sensitive information, monitor threats, and respond effectively to cyber incidents. Especially for SMEs, the strategic investment in these technologies is vital to achieving Cybersecurity Maturity since they have less money to spend than multinationals (Alahmari & Duncan, 2021).

According to Golightly et al. (2023), access management of software and sensitive information is a crucial element of a robust cybersecurity strategy. Technologies like role-based access control and multi-factor authentication help ensure that only authorized personnel can access critical systems and data, reducing the risk of insider threats and unauthorized breaches.

Maintaining system security is essential to address vulnerabilities in software and hardware (Dissanayake et al., 2021). Unpatched systems are a common attack vector cybercriminals exploit to gain unauthorized access or execute malicious code. Regular updates to software, operating systems, and applications reduce the risk of exploitation and contribute to maintaining compliance with industry standards. Furthermore, robust backup systems are essential for a good cybersecurity posture, providing resilience against data loss in case of ransomware or hardware failures (Ali et al., 2015).

2.2.2 Competitive Advantage

Competitive Advantage is a foundational concept in strategic management, as it provides insight into the factors that drive the differences in performance between enterprises (Zott & Amit, 2008). At its core, Competitive Advantage represents the unique attributes and capabilities that enable a firm to achieve superior performance compared to its competitors.

Despite the prominence of the term Competitive Advantage in both academia and practice, it remains a source of confusion due to the abundance of varying definitions and interpretations (Sigalas, 2015). To address this issue, this thesis emphasizes the critical dimensions of Competitive Advantage: customer trust, differentiation from competition, operational resilience, continuity, and thus availability. By grounding Competitive Advantage in these pillars, the research aims to provide a practical and actionable construct for understanding how SMEs can leverage these attributes to achieve Competitive Advantage.

Customer Trust

Customer trust is a pivotal element of Competitive Advantage, especially in the digital ecosystem where data privacy concerns and security breaches are prevalent (Mmango & Gundu, 2024). A company's ability to demonstrate its commitment to cybersecurity acts as a trust signal, reassuring customers that their data is handled securely and responsibly. This builds confidence among customers, fostering loyalty and long-term relationships. Trust cultivated in this manner will strengthen customer retention and reinforce the reputation of the enterprise as a secure and dependable partner.

Operational Continuity and Resilience

Operational continuity and resilience reflect an enterprise's ability to maintain and quickly recover critical operations during and after disruptions (Al-Hawamleh, 2024). Cybersecurity is essential in enabling this resilience, enabling enterprises to withstand and adapt to cyber threats while minimizing losses and downtime. Enterprises that exhibit strong operational resilience reassure stakeholders and customers and develop themselves as reliable business partners in the business ecosystem (Otola et al., 2023).

Differentiation from Competition

Differentiation involves creating unique value propositions that set a company apart from its competitors. In the context of cybersecurity, enterprises can differentiate themselves from their competitors by employing cybersecurity specialists and using features like advanced encryption,

multi-factor authentication, or blockchain-based security solutions (Alahmari & Duncan, 2021; Golightly et al., 2023). Additionally, emphasizing proactive security measures, such as real-time threat detection and automated incident response systems, further sets these companies apart from competitors who may adopt only reactive approaches to cybersecurity (Keskin et al., 2021).

Integration of Dimensions

The interplay of customer trust, operational continuity and resilience, and differentiation underscores a holistic approach to Competitive Advantage. In the context of cybersecurity, these dimensions highlight how SMEs can build a robust market position, foster long-term growth, and mitigate risks associated with operational disruptions (Kosutic, 2021).

2.2.3 Regulatory Compliance

Since cyber threats keep evolving, governments and regulating bodies have decided to get involved by creating cybersecurity regulations. These regulations play a crucial role in shaping the cybersecurity landscape for SMEs. They aim to protect sensitive data, ensure business continuity, and maintain customer trust.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) has been implemented by the European Union in 2018. It is the most comprehensive data protection regulation that is affecting European SMEs. The GDPR mandates that all organizations implement appropriate technical and organizational measures to ensure the security of personal data (European Parliament & Council of the European Union, 2016). This means that SMEs must be protected against unauthorized access, accidental loss, destruction, or damage. Furthermore, GDPR requires SMEs to conduct regular risk assessments to identify vulnerabilities in their data processing activities and to address them accordingly. Data collection should be minimized, meaning that only necessary data should be collected, and the data should only be used for specified purposes. The GDPR also states that SMEs should establish data retention policies to ensure that personal data is not kept longer than necessary.

According to the GDPR, SMEs must maintain detailed records of their data processing activities and implement comprehensive data protection policies (European Parliament & Council of the European Union, 2016). This requires an investment by the SMEs in their systems and practices that ensure compliance with the GDPR standards. Depending on the nature of the data processing activities, SMEs will be required to appoint a Data Protection Officer to oversee compliance with the GDPR.

If an SME suffers a data breach, the GDPR mandates it to notify the relevant data protection authorities within 72 hours of discovering the breach (European Parliament & Council of the European Union, 2016). The SME must also inform the affected individuals if the breach will likely result in a high risk to their rights and freedom.

Not complying with the GDPR can result in fines up to €20 million or 4% of their annual global

turnover, whichever is higher (European Parliament & Council of the European Union, 2016). The GDPR imposes these stringent fines for non-compliance to ensure that organizations take data protection seriously.

Network and Information Systems 2 (NIS2) Directive

The Network and Information Systems 2 (NIS2) Directive, another regulation implemented by the European Union, aims to enhance cybersecurity across member states (European Union, 2022). Unlike the GDPR, which primarily focuses on personal data protection, NIS2 targets organizations that are critical to supply chains essential for societal and economic activities. These include sectors such as energy, banking, and public administration.

NIS2 encompasses a broader range of cybersecurity practices than the GDPR (European Union, 2022). It requires organizations to implement comprehensive cybersecurity risk management measures and to ensure the security of their network and information systems. This directive mandates that the relevant authorities must be notified within 24 hours of detecting a cybersecurity incident. This fast reporting is crucial for mitigating the impact of incidents and enhancing the overall security posture of critical infrastructure.

Furthermore, NIS2 encourages SMEs to participate in information-sharing networks (European Union, 2022). These networks facilitate the exchange of threat intelligence and best practices between organizations and authorities. In this collaborative environment, SMEs can improve their cybersecurity defenses and contribute to a more resilient digital ecosystem.

2.3 Relationship between the Constructs

This section examines the theoretical relationships among Cybersecurity Maturity, Competitive Advantage, regulatory compliance, and the frequency of cyber incidents. Drawing on prior literature, the hypotheses are developed to understand how these constructs interact to influence organizational outcomes.

H1: Cybersecurity Maturity has a direct and positive effect on Competitive Advantage

Existing literature states that having good Cybersecurity Maturity will protect the existing intellectual property and knowledge of an enterprise, and by increasing customer trust, it will sustain an enterprise's Competitive Advantage (Kosutic, 2021; Lloyd, 2020; Mmango & Gundu, 2024). When an enterprise showcases its commitment to cybersecurity, it sends a clear signal that it values customer privacy and is dedicated to safeguarding sensitive information. This assurance fosters a sense of reliability and reduces perceived risks associated with engaging with the business. Over time, this trust strengthens customer loyalty, which is a critical component of sustained Competitive Advantage.

Research indicates that robust cybersecurity practices can be a key differentiator for SMEs, particularly in industries where such measures are often overlooked. Many SMEs focus on cost reduction and operational efficiency, sometimes at the expense of comprehensive cybersecurity

strategies (Chidukwani et al., 2022). This gap allows security-conscious SMEs to stand out by offering safer products, services, and business environments (Hasani et al., 2023). By making proactive investments in cybersecurity, these SMEs can position themselves as more reliable and lower-risk partners, which in turn makes them more attractive to customers.

Cybersecurity maturity can create differentiation opportunities, such as the ability to collaborate with larger enterprises (Lloyd, 2020). Larger enterprises are increasingly more interested in the cybersecurity posture of the smaller enterprises they want to cooperate with. SMEs with strong Cybersecurity Maturity are better positioned to meet the stringent security expectations of these organizations. This mitigates potential risks for larger companies and fosters trust in collaborative ventures. SMEs that proactively invest in cybersecurity gain a competitive edge over less-prepared competitors, making them more attractive business partners and increasing their chances of securing lucrative contracts.

Moreover, Cybersecurity Maturity plays a pivotal role in ensuring business continuity and resilience (Al-Hawamleh, 2024; Altaha & Hafizur Rahman, 2023). By implementing robust cybersecurity measures, enterprises can safeguard their operations against potential disruptions caused by cyberattacks, data breaches, or system failures. Minimizing downtime, protecting critical business processes, and ensuring that the organization can continue to operate effectively, even in the face of unforeseen challenges. This ability to maintain stable operations, even under cyber threats, further differentiates SMEs from competitors who may struggle with disruptions, reinforcing their reputation as a reliable company.

H2: Regulatory Compliance is a mediating variable in the relationship between Cybersecurity Maturity and Competitive Advantage

Next to the direct effect of Cybersecurity Maturity on Competitive Advantage, we hypothesize that Cybersecurity Maturity also enhances Competitive Advantage indirectly through regulatory compliance. Cybersecurity Maturity reflects an organization's ability to implement effective cybersecurity practices across the dimensions people, processes, and technology. A higher level of Cybersecurity Maturity typically results in more structured security policies, improved risk management, and better alignment with regulatory requirements (Koolen et al., 2024). Organizations with mature cybersecurity capabilities are more likely to have well-defined procedures for data protection, incident response, and access control, all of which facilitate adherence to regulatory standards such as the GDPR and the NIS2 Directive (European Parliament & Council of the European Union, 2016; European Union, 2022). These factors suggest that higher Cybersecurity Maturity leads to improved regulatory compliance, as organizations with mature cybersecurity practices are better equipped to meet legal and industry standards efficiently and consistently.

Regulatory compliance, in turn, could strengthen an organization's competitive position. Adhering to cybersecurity regulations signals a strong commitment to privacy and data security, which is essential for building trust with customers, partners, and stakeholders (Tikkinen-Piri et al., 2018). Additionally, regulatory compliance can serve as a differentiation factor in com-

petitive markets. Organizations that successfully meet or exceed regulatory requirements may be perceived as more reliable and secure, leading to Competitive Advantage (Vives, 2019).

H3: Frequency of Cyber Incidents is a mediating variable in the relationship between Cybersecurity Maturity and Competitive Advantage

A high level of Cybersecurity Maturity significantly reduces the frequency and impact of successful cyber incidents (Dinkova et al., 2023). By implementing advanced cybersecurity practices, enterprises can better identify, prevent, and mitigate potential threats, decreasing the likelihood of data breaches, ransomware attacks, or other malicious activities. Reducing cyber incidents ensures smoother business operations and minimizes disruptions that can arise from cybersecurity challenges.

Furthermore, the frequency of cyber incidents directly impacts customer trust (Bajwa et al., 2023). Customers are increasingly aware of cyber risks and tend to avoid businesses with a history of data breaches or inadequate cybersecurity measures. By demonstrating robust cybersecurity practices and maintaining a track record of few or no security incidents, enterprises can foster trust and strengthen their relationships with customers.

2.4 A Conceptual Model of Cybersecurity and Competitive Advantage

This section summarizes and visualizes the relationships between the constructs previously discussed, providing a structured overview of how Cybersecurity Maturity drives Competitive Advantage in SMEs. As illustrated in Figure 1, the framework integrates direct and mediated pathways, summarizing the critical relationships:

- Direct Relationship:
  - Cybersecurity Maturity directly enhances Competitive Advantage by building trust, ensuring operational continuity, and enabling differentiation.
- Mediated Relationships:
  - Through Regulatory Compliance: Regulatory adherence, enabled by Cybersecurity Maturity, supports trust-building and market positioning.
  - Through Frequency of Cyber Incidents: Cybersecurity Maturity minimizes disruptions, protecting the enterprise's reputation, reliability, and customer trust.

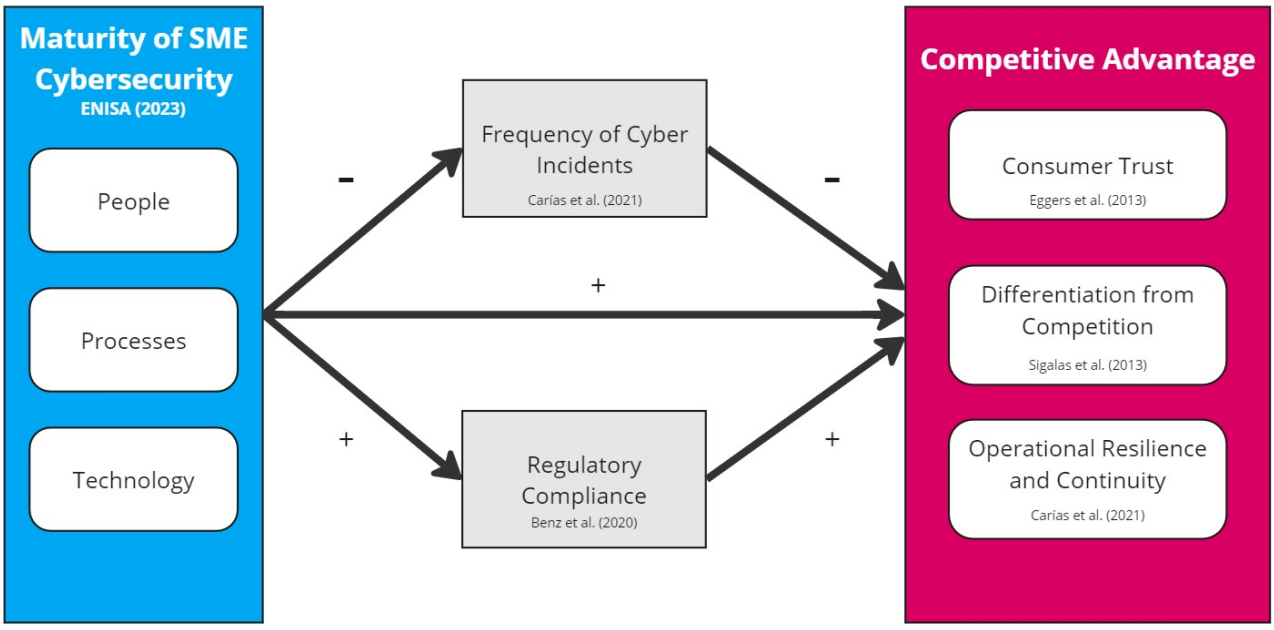

Figure 1: Theoretical Framework and Literature on Construct Assessment

3 Methodology

This section outlines the methodology employed to investigate the relationship between Cybersecurity Maturity and Competitive Advantage in SMEs. The research adopts a non-experimental, correlational, cross-sectional survey design to assess how Cybersecurity Maturity, Competitive Advantage, regulatory compliance, and the frequency of cyber incidents are interrelated. Figure 2 depicts a schematic overview of the methods applied in this research.

The study focuses on SMEs, with data collected from individuals knowledgeable about their organizations' cybersecurity practices and competitive positioning. A sample of at least 30 SMEs was targeted using a combination of convenience and purposeful sampling methods. The key constructs were operationalized through validated survey instruments, and data was collected through an online self-assessment survey using 5-point Likert scale questions.

The data was analysed using Partial Least Squares Structural Equation Modeling (PLS-SEM) in ADANCO, focusing on testing the direct and mediated relationships between Cybersecurity Maturity and Competitive Advantage. The methodology also includes strategies for assessing construct validity, model fit, and hypothesis testing, ensuring robust analysis of the proposed relationships. Finally, potential limitations of the methodology are addressed.

3.1 Research Design

This research adopts a non-experimental, correlational, cross-sectional survey design. A non-experimental approach was chosen for this study as it focuses on measuring variables without researcher intervention (Patten & Newhart, 2023). This allows the researcher to observe how the key factors in this research are connected without intervening in the operations of the SMEs.

This correlational study focuses on examining relationships between variables, particularly the degree to which they influence one another. Correlational research designs are used for studies that aim to predict outcomes or explain relationships among variables (Creswell, 2017). Specifically, this research employs an exploratory correlational design, which is ideal for understanding associations between variables and identifying patterns of influence.

Additionally, this study utilizes a cross-sectional survey design, where data is collected at a single point in time. Creswell (2017) highlights that cross-sectional designs effectively capture current attitudes, perceptions, or behaviours. This approach aligns with this study's objective of understanding Cybersecurity Maturity, Competitive Advantage, and possible related mediating factors within SMEs.

3.2 Population and Sample

The population for this study consists of SMEs. To determine whether an enterprise qualifies as an SME, this research adopts the European Commission's definition: "The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an

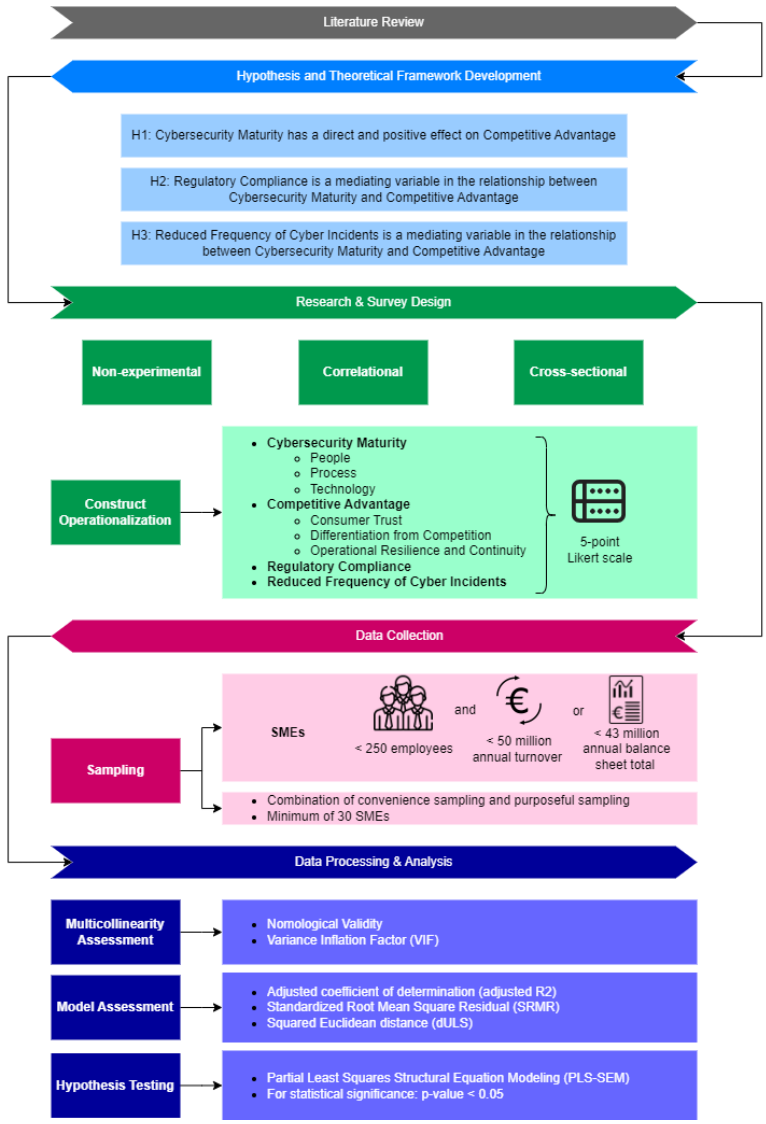

Figure 2: Schematic Overview of the Research Methodology

annual balance sheet total not exceeding EUR 43 million" (EC, 2003). The target respondents for the survey are individuals with knowledge about their SME's Cybersecurity Maturity and Competitive Advantage, such as directors, managers, or IT personnel.

This research employs non-probability sampling techniques to recruit participants, precisely a combination of convenience and purposeful sampling. Convenience sampling allows for the inclusion of readily available participants, while purposeful sampling ensures the selection of respondents with specific knowledge of cybersecurity and Competitive Advantage within their SME (Ahmed, 2024).

The goal for the sample size for this study was determined to be a minimum of 30 participating SMEs. This number was determined by balancing both resource constraints and statistical considerations. Resource constraints are a common reason for limiting the amount of data expected to be collected (Lakens, 2022). Given the limitations in time and resources, recruiting a much larger sample was deemed not feasible. However, to ensure the validity of the findings, the researcher aimed to meet the minimum threshold required for meaningful statistical analysis.

The Central Limit Theorem (CLT) was a guiding principle in this decision, as it suggests that a sample size of at least 30 is sufficient to approximate a normal distribution for many statistical techniques (Islaqm, 2018; Kwak & Kim, 2017). By targeting a sample size of at least 30 SMEs, this study tries to ensure the robustness of inferential analyses while working with the available resources.

3.3 Construct Operationalization

In this study, the key constructs are operationalized using survey items adopted and adjusted from existing validated tools. The survey utilized a 5-point Likert scale for items measuring the key constructs, allowing respondents to indicate their level of agreement or perception. This approach provided a standardized method for measuring the constructs of Cybersecurity Maturity, Competitive Advantage, regulatory compliance, and the frequency of cyber incidents.

Each construct is divided into specific dimensions that address different parts of the construct, as shown in Table 1. The full survey can be seen in Appendix 6.

Table 1: Constructs, Dimensions, and Items used in the Study.

Construct	**Dimension**	**Items**
Cybersecurity Maturity	People	"Cybersecurity training and awareness are managed effectively in my company." "Privileged users in my company understand their cybersecurity roles and responsibilities." "My company has effective policies to protect private data." "My company coordinates cybersecurity roles with internal and external partners." "Cybersecurity awareness campaigns are conducted regularly in my company." "Employees are encouraged to report any security incidents or concerns."
Cybersecurity Maturity	Process	"My company assesses cybersecurity risks when selecting external partners." "Response and recovery plans are regularly tested and understood by personnel." "Cybersecurity risks are integrated into our governance and risk management processes." "My company identifies and manages cybersecurity risks in the supply chain." "My company regularly reviews and updates incident response plans."

Construct	Dimension	Items
Cybersecurity Maturity	Technology	"Access to software and sensitive information is well managed in my company." "Data leak prevention measures are in place in my company." "Software and systems are updated and patched promptly in my company." "Configuration and change control processes are followed in my company." "We have real-time monitoring and response systems for cybersecurity threats." "Backup systems are in place to ensure data recovery."
Frequency of Cyber Incidents	-	"Our cybersecurity policies and procedures have led to a reduction in the number of cybersecurity incidents." "Our organization experiences fewer cyber incidents than our industry competitors."
Competitive Advantage	Customer Trust	"Our customers express high levels of satisfaction with our brand." "Complaints about our products/services are rare." "Customers frequently return for repeat purchases." "Our customer base is loyal and consistently chooses us."
Competitive Advantage	Differentiation from Competition	"Our products/services are unique compared to competitors." "We offer features or benefits that are hard for competitors to replicate." "Our offerings are perceived as more innovative than competitors'." "Our brand identity sets us apart from competitors." "Our business is recognized for pioneering new ideas."
Competitive Advantage	Operational Resilience and Continuity	"Employees know the steps needed to maintain critical assets during incidents." "My company has documented recovery plans with time and point objectives." "My business' continuity plans are regularly tested and updated."
Regulatory Compliance	-	"My company is aware of laws and regulations affecting our cybersecurity practices." "My company has taken necessary actions to comply with GDPR." "My company has taken actions to comply with the NIS2 Directive." "My company has conducted compliance audits for cybersecurity regulations."

3.3.1 Cybersecurity Maturity

The Cybersecurity Maturity construct is operationalized across three dimensions: people, process, and technology. Each dimension is operationalized through multiple survey items to capture the different aspects that correspond to that dimension:

- **People**: This dimension assesses the human element in cybersecurity, focusing on employee awareness, training, and roles related to cybersecurity within the SME.
- **Process**: This dimension measures the organization's approach to cybersecurity processes, including risk assessment, response planning, and supply chain monitoring.
- **Technology**: This dimension focuses on the technological tools and infrastructure SMEs use to secure their digital environments.

The items used to measure these dimensions are adapted from the European Union Agency for Cybersecurity's (ENISA) Cybersecurity Maturity Assessment for Small and Medium Enterprises, which provides a comprehensive framework for evaluating Cybersecurity Maturity in SMEs.

3.3.2 Competitive Advantage

Competitive Advantage is operationalized through customer trust, differentiation from competition, and operational resilience and continuity.

- **Customer Trust**: This dimension evaluates how SMEs perceive customer loyalty and whether customers are satisfied with the services offered. The dimension will reflect the average trust of customers in the services of the SME.
- **Differentiation from Competition**: This dimension assesses whether the SME is able to differentiate itself from its competitors, for example, in being more secure or innovative.
- **Operational Resilience and Continuity**: This dimension measures the SME's ability to maintain operational continuity during and after cybersecurity incidents.

These dimensions are measured using survey items adapted from Carias et al. (2021), Eggers et al. (2013), and Sigalas et al. (2013), which explore SMEs' self-assessment capabilities regarding various aspects of Competitive Advantage. Consequently, in this research, SMEs will assess these dimensions themselves, following the methodology of the aforementioned studies.

3.3.3 Frequency of Cyber Incidents and Regulatory Compliance

The two theorized mediating factors between Cybersecurity Maturity and Competitive Advantage, the frequency of cyber incidents and regulatory compliance, are operationalized using tools developed by Benz and Chatterjee (2020). These tools are specifically tailored to the SME context, addressing the unique challenges these organizations face in managing cybersecurity risks and adhering to regulatory standards.

The frequency of cyber incidents is measured through two items that capture the occurrence and severity of cybersecurity events within the SME over the past year. This construct reflects the effectiveness of an SME's cybersecurity practices, its ability to detect cybersecurity attacks, and its ability to mitigate threats.

Regulatory compliance, on the other hand, assesses an SME's adherence to pertinent cybersecurity laws and frameworks. This construct is operationalized through four survey items, specifically addressing compliance with key regulations such as the NIS2 Directive and the GDPR.

By capturing these mediating factors, this study examines how the relationship between Cybersecurity Maturity and Competitive Advantage is influenced by the ability to reduce cyber incidents and achieve regulatory compliance. These constructs will enable the researcher to understand the broader implications of cybersecurity practices within SMEs.

3.4 Data Collection

Data for this study was collected through an online self-assessment survey hosted on Qualtrics. The survey link was distributed through three main channels: social media platforms (e.g., LinkedIn), direct outreach, and a poster presentation at a cybersecurity symposium. These channels were chosen for their relevance and ability to reach the target demographic of SMEs and their representatives.

Respondents were informed that participation was voluntary to encourage participation and ensure ethical standards were met, and they could withdraw at any time. Additionally, they were reassured that all responses would remain anonymous and confidential.

A cybersecurity specialist reviewed and validated the survey. This expert review helped ensure the survey's relevance, clarity, and alignment with the study's objectives, improving the quality and accuracy of the survey questions and their suitability for the target audience.

Respondents were recruited through the previously mentioned channels. After removing responses from "speeders" and "straightliners," the final sample consisted of 46 valid responses. "Speeders" are respondents who complete the survey unusually quickly, often without carefully reading the questions or providing thoughtful answers (Zhang & Conrad, 2014). Speeding can be problematic because it leads to unreliable data, which can skew the results. In this study, speeders were excluded based on the following cutoff formula:

$$Cutoff = \text{median of completion time} * 75\% \tag{1}$$

Straightlining is the phenomenon where survey respondents give (nearly) identical answers to items of questions, this may reduce the quality of the data (Kim et al., 2018). Straighliners were removed based on visual inspection. Visual inspection is a method of dealing with straightliners where, through manual inspection, identical or highly similar answers across a range of questions can be removed (Meade & Craig, 2012).

3.5 Data Analysis

The data collected for this study were analysed using ADANCO, a software specifically designed for Partial Least Squares Structural Equation Modeling (PLS-SEM) (Henseler, 2017b). PLS-SEM is a variance-based structural equation modeling technique that estimates relationships between latent variables by maximizing the explained variance of dependent constructs (Hair et al., 2022). PLS-SEM was selected because it is well-suited for exploratory research and can effectively model complex relationships between constructs, even with smaller sample sizes (Kante & Michel, 2023). ADANCO allows researchers to perform a variety of statistical procedures, including testing for reliability indicators, multicollinearity, and structural equation models (Henseler, 2017b).

3.5.1 Composite Model

Since this study exclusively uses emergent variables, the model is categorized as a composite model, as outlined by Yu et al. (2021). A composite model is defined by constructs that are formed by combining their indicators rather than being represented as latent variables derived from underlying constructs. Figure 3 shows the composite model used in this research.

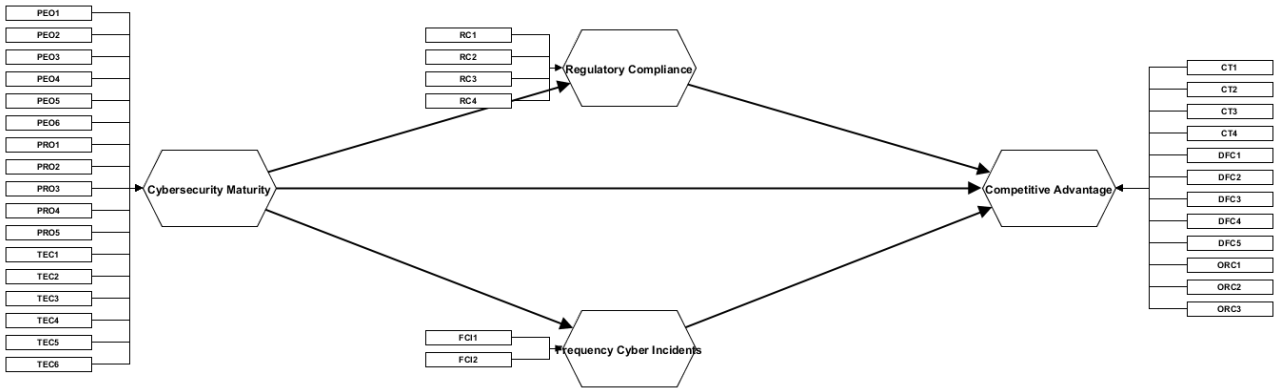

Figure 3: Composite Model with Theorized Pathways Between Constructs

This model explores the direct relationship between Cybersecurity Maturity and Competitive Advantage. It also examines the mediated relationships through two pathways: first, via the frequency of cyber incidents, and second, through regulatory compliance. These mediating constructs are also treated as emergent variables, and the study investigates the relationships between them and Cybersecurity Maturity to understand how they influence an SME's Competitive Advantage.

3.5.2 Construct, Discriminant, and Convergent Validity

The assessment of construct, discriminant, and convergent validity for emergent constructs differs from that of latent constructs. This is because composite models impose fewer restrictions on the overall model (Henseler, 2017a). In this study, the validity of the measurement model was evaluated through the lens of nomological validity, which examines the relationships between constructs and assesses multicollinearity among indicators using the variance inflation factor (VIF).

Nomological Validity
Nomological validity assesses whether the constructs perform as expected within the theoretical framework. Composite constructs' validity depends on the relationships they share with other constructs in the structural model.

In this study, the structural relationships between constructs were examined to ensure they aligned with theoretical predictions. The path coefficients for the composite constructs were evaluated for significance using bootstrapping techniques. Additionally, the R^2 values for endogenous constructs were assessed to ensure that the predictors, including the composite constructs, contributed meaningfully to explaining the variance in the model.

Variance Inflation Factor (VIF)
Multicollinearity among the indicators of composite constructs was assessed by calculating VIF values. A high VIF indicates redundancy among the indicators, which can negatively affect the interpretability and stability of the composite construct.

The threshold of the VIF values of 3.3 ensures that the indicators are sufficiently distinct and do not exhibit problematic multicollinearity (Hair et al., 2009). Any indicators with VIF values exceeding 3.3 and showing a high degree of redundancy were removed to mitigate multicollinearity issues.

This process ensures that the indicators reflect unique aspects of their respective composite constructs and contribute effectively to their operationalization.

3.5.3 Assessment of Model Fit and Hypothesis Testing

To evaluate the model and test the hypotheses, several statistical measures were applied. The primary focus was on assessing the path coefficients between the constructs, determining the significance of the relationships using p-values, and assessing the model fit.

Model Assessment
The model's fit and power were evaluated using multiple fit indices, including the adjusted coefficient of determination (adjusted R^2), Standardized Root Mean Square Residual (SRMR), and the squared Euclidean distance (d_{ULS}).

The adjusted R^2 value quantifies the amount of variance in the dependent variable explained by the independent variables, with higher values indicating a better model fit and greater predictive power. The adjusted R^2 also considers the number of predictors and mitigates the risk of overfitting.

Additionally, the SRMR measures the difference between the observed and predicted correlations, where lower SRMR values indicate a better fit. An SRMR value below 0.10 indicates an acceptable model fit (Kline, 2011).

The squared Euclidean distance (d_{ULS}) is indicative of the difference between the model-implied and observed covariance matrices. Lower values suggest a more accurate model fit (Ringle et

al., 2024). The combination of these indices helps assess both the model's explanatory power and its overall goodness-of-fit.

Hypothesis Testing
For hypothesis testing, p-values were used to assess the significance of the relationships proposed in the model. The hypotheses were tested by examining the path coefficients between constructs, which were obtained through PLS-SEM analysis in ADANCO. A p-value lower than the conventional threshold of 0.05 was considered statistically significant.

The p-values were computed for each path in the structural model to determine whether the hypothesized effects were supported by the data gathered from the survey. Based on these p-values, conclusions regarding the acceptance or rejection of each hypothesis were drawn.

3.6 Potential Limitations

While this methodology will provide valuable insights into the relationship between Cybersecurity Maturity, Competitive Advantage, and regulatory compliance, several limitations should be considered when interpreting the results.

Firstly, the sample size, though sufficient for the statistical analyses with at least 30 SMEs, may limit the generalizability of the findings (Hair et al., 2022). A larger sample would allow for a more comprehensive understanding of the complex relationships among the constructs, especially within the diverse population of SMEs.

Secondly, the sampling methods, convenience and purposeful sampling, introduce potential biases (Etikan, 2016). This may cause the results of this study to not fully represent the broader SME population, as it primarily targeted participants with specific expertise in cybersecurity and Competitive Advantage. Whereas SMEs may not necessarily employ someone with cybersecurity expertise.

The study also relied on self-reported data, which could introduce bias (Podsakoff et al., 2003). Respondents may have been influenced by social desirability or not accurately assessed their organization's cybersecurity practices or competitive positioning. This could lead to overestimations or underestimations of their SME's maturity, advantage, or regulatory compliance, thus impacting the reliability of the data.

4 Results

This section presents the findings of the study, structured as follows. First, the demographic characteristics of the responding SMEs are described to provide context for the sample. Next, the results of the multicollinearity assessment are outlined, ensuring the validity of the indicators used in the measurement model. Following this, the structural model's model fit and explanatory power are evaluated, including goodness-of-fit indices and adjusted R^2 values. Finally, the relationships between constructs are analysed through inference statistics, providing insights into the direct, indirect, and total effects within the model.

4.1 Descriptive Statistics

Table 2 summarizes the demographic characteristics of the responding SMEs. 46 SMEs answered the survey adequately. The majority of the respondents represent SMEs in the services sector (43.5%), followed by other industries (21.7%) and retail (19.6%). The technology sector accounts for 13% of the sample, while the manufacturing sector represents the smallest group at 2.2%.

Regarding annual revenue, most SMEs in the sample (82.6%) report earnings of less than €10 million. A smaller proportion of respondents report revenues between €10 million and €30 million (10.9%), while only 6.5% report revenues between €30 million and €50 million.

The majority of SMEs employ 2 to 50 employees (69.6%), consistent with the typical size range for small businesses. SMEs with 51 to 150 employees make up 17.4% of the sample, while single-employee SMEs account for 8.7%. Only 4.3% of the sample consists of SMEs at the larger end of the scale, employing 151 to 250 employees.

Table 3 presents the descriptive statistics for the survey items assessing SMEs' perceived cybersecurity maturity across three dimensions: people (PEO), process (PRO), and technology (TEC). The people dimension, which evaluates the effectiveness of cybersecurity training, awareness, and incident reporting, has mean values ranging from 2.52 (SD = 1.26) to 3.70 (SD = 1.16). These results suggest that while some SMEs believe their employees are well-informed and encouraged to report security concerns, others perceive gaps in training and awareness programs.

The process dimension focuses on risk management, incident response planning, and supply chain security. Mean values in this category range from 2.91 (SD = 0.97) to 3.15 (SD = 1.18), indicating moderate confidence in SMEs' cybersecurity governance and risk management efforts. The variability in responses suggests that some organizations have structured cybersecurity processes, while others may lack regular assessments and updates.

The technology dimension assesses access control, data protection, system updates, and real-time monitoring capabilities. Mean values in this category range from 3.04 (SD = 1.12) to 3.65 (SD = 0.91), indicating a slightly more favourable perception of cybersecurity infrastructure compared to people and process aspects. This category's relatively lower standard deviations

Table 2: The Demographic Characteristics of the participating SMEs.

Variable	N (46 total)	%
Industry Sector		
Manufacturing	1	2.2
Retail	9	19.6
Services	20	43.5
Technology	6	13
Other	10	21.7
Annual Revenue		
Less than €10 million	38	82.6
Between €10 million and €30 million	5	10.9
Between €30 million and €50 million	3	6.5
Amount of Employees		
1	4	8.7
2 - 50	32	69.6
51 - 150	8	17.4
151 - 250	2	4.3

suggest more consistency in SMEs' responses, implying that technical security measures may be more uniformly implemented than training and governance practices.

Table 3: Descriptive Statistics for Survey Items Corresponding to Cybersecurity Maturity

Survey Item	**Mean (SD)**	**Survey Item**	**Mean (SD)**	**Survey Item**	**Mean (SD)**
PEO1	3.00 (1.32)	PRO1	3.13 (1.15)	TEC1	3.65 (0.91)
PEO2	3.26 (0.99)	PRO2	3.02 (1.15)	TEC2	3.54 (0.90)
PEO3	3.54 (1.14)	PRO3	3.07 (1.07)	TEC3	3.50 (0.90)
PEO4	3.09 (1.10)	PRO4	2.91 (0.97)	TEC4	3.37 (1.10)
PEO5	2.52 (1.26)	PRO5	3.15 (1.18)	TEC5	3.04 (1.12)
PEO6	3.70 (1.16)			TEC6	3.54 (1.04)

Table 4 presents the descriptive statistics for the survey items assessing SMEs' perceived competitive advantage across three dimensions: customer trust (CT), differentiation from competition (DFC), and operational resilience and continuity (ORC).

The customer trust dimension, which measures customer satisfaction, loyalty, and brand perception, has mean values ranging from 3.19 (SD = 0.82) to 4.04 (SD = 0.80). The relatively high mean scores suggest that SMEs generally perceive strong customer trust, particularly in terms of customer satisfaction and repeat purchases. The standard deviations indicate a moderate level of variation, implying that some firms experience higher customer trust than others.

The differentiation from competition dimension assesses how SMEs perceive their uniqueness and market positioning. The mean scores range from 3.50 (SD = 0.77) to 3.87 (SD = 1.04), suggesting that most SMEs believe they offer distinctive and innovative products or services. However, the standard deviations indicate some variation in how strongly businesses perceive their competitive differentiation, possibly reflecting differences in industry sectors or strategic focus.

The operational resilience and continuity dimension evaluates SMEs' preparedness for maintaining critical operations during disruptions. The mean values range from 3.13 (SD = 0.82) to 3.35 (SD = 0.77), indicating a moderate level of confidence in business continuity measures. The lower standard deviations suggest that perceptions of resilience are relatively consistent among SMEs.

Table 4: Descriptive Statistics for Survey Items Corresponding to Competitive Advantage

Survey Item	**Mean (SD)**	**Survey Item**	**Mean (SD)**	**Survey Item**	**Mean (SD)**
CT1	3.19 (0.82)	DFC1	3.59 (0.80)	ORC1	3.35 (0.77)
CT2	4.04 (0.80)	DFC2	3.54 (0.99)	ORC2	3.30 (0.89)
CT3	3.93 (0.88)	DFC3	3.87 (1.04)	ORC3	3.13 (0.82)
CT4	3.91 (0.90)	DFC4	3.50 (0.77)		
		DFC5	3.87 (0.81)		

Table 5 presents the descriptive statistics for regulatory compliance (RC) and frequency of cyber incidents (FCI). The RC items, which measure SMEs' perceived compliance with cybersecurity regulations, have mean values between 3.26 (SD = 1.02) and 3.39 (SD = 1.03), indicating moderate confidence in regulatory adherence. The FCI items, measuring how frequently SMEs experience cyber incidents, range from 3.04 (SD = 0.82) to 3.54 (SD = 0.80). This suggests that most SMEs perceive their cybersecurity policies and procedures as effective in reducing cyber incidents and believe they experience fewer incidents than their industry competitors.

Table 5: Descriptive Statistics for Survey Items Corresponding to Regulatory Compliance and Frequency of Cyber Incidents

Survey Item	**Mean (SD)**	**Survey Item**	**Mean (SD)**
RC1	3.35 (1.07)	FCI1	3.54 (0.80)
RC2	3.26 (1.02)	FCI2	3.04 (0.82)
RC3	3.35 (1.02)		
RC4	3.39 (1.03)		

4.2 Multicollinearity Assessment

Table 6 presents the VIF value for each survey item, organized by the constructs of the model. The VIF values assess multicollinearity among indicators within their respective constructs. The abbreviations in the table stand for people (PEO), process (PRO), technology (TEC), fre-

quency of cyber incidents (FCI), customer trust (CT), differentiation from competition (DFC), operational resilience and continuity (ORC), and regulatory compliance (RC).

For the **Cybersecurity Maturity** construct, VIF values range from 1.5563 (PEO2) to 4.3271 (PRO5), with most indicators falling below the commonly accepted threshold of 3.3. For the **Frequency of Cyber Incidents** construct VIF values for FCI1 and FCI2 are identical at 1.2109. In the **Competitive Advantage** construct, the VIF values range from 1.8836 (CT2) to 3.4977 (CT4), while the **Regulatory Compliance** construct has VIF values between 1.8570 (RC1) and 2.4208 (RC2).

The survey items with VIF values higher than the threshold of 3.3 were reassessed on their nomological validity. This meant that PRO3, PRO5, TEC3, and CT4 were deleted from the model to safeguard against multicollinearity.

The rest of the VIF values fall within acceptable ranges, supporting the absence of significant multicollinearity issues in the measurement model. These results validate the indicators' suitability for further analysis in the structural equation model.

Table 6: The Variance Inflation Factor Values per Survey Item

Indicator	Competitive Advantage	Frequency of Cyber Incidents	Cybersecurity Maturity	Regulatory Compliance
PEO1			2.2767	
PEO2			1.5563	
PEO3			2.3891	
PEO4			1.9551	
PEO5			2.7292	
PEO6			2.3848	
PRO1			2.2945	
PRO2			2.9410	
PRO3			3.5520	
PRO4			2.6275	
PRO5			4.3271	
TEC1			1.8256	
TEC2			2.5821	
TEC3			3.8089	
TEC4			2.3372	
TEC5			2.6035	
TEC6			2.4261	
FCI1		1.2109		
FCI2		1.2109		
CT1	2.9372			
CT2	1.8836			
CT3	3.0991			
CT4	3.4977			
DFC1	3.2533			
DFC2	2.6184			
DFC3	2.4040			
DFC4	1.4878			
DFC5	2.2624			
ORC1	2.4535			
ORC2	2.8235			
ORC3	2.3062			
RC1				1.8570

Indicator	Competitive Advantage	Frequency Cyber Incidents	Cybersecurity Maturity	Regulatory Compliance
RC2				2.4208
RC3				2.0007
RC4				2.0135

4.3 Model Fit and Explanatory Power

Table 7 presents the goodness of model fit for the estimated model. The model fit is assessed using the SRMR and d_{ULS}.

Table 7: Goodness of Model Fit (Estimated Model)

Fit Index	Value	HI95	HI99
SRMR (Standardized Root Mean Square Residual)	0.0951	0.0917	0.1013
d_{ULS} (Squared Euclidean Distance)	4.4897	4.1723	5.0913

The observed SRMR value is 0.0951, with the bootstrap-based 95% (HI95) SRMR value being 0.0917 and the bootstrap-based 99% (HI99) SRMR value being 0.1013. This indicates that the model's fit is acceptable at a 95% confidence level. Generally, SRMR values below 0.08 are considered indicative of a good model fit, so the observed SRMR is slightly above the desired threshold, suggesting that while the model fits well, there may still be some room for improvement. SRMR values below 0.10 are considered an acceptable fit.

The observed value for d_{ULS} is 4.4897, the bootstrap-based 95% (HI95) d_{ULS} value being 4.1723 and the bootstrap-based 99% (HI99) d_{ULS} value being 5.0913. Because the observed d_{ULS} falls within the H95-H99 interval, the model can be considered an acceptable fit based on this criterion.

The adjusted R^2 values for the endogenous constructs in the model are presented in Table 8. These values indicate the part of the variance in each endogenous construct that is explained by the independent variables after adjusting for model complexity.

Table 8: R-Squared Values for the Endogenous Constructs

Construct	R^2	Adjusted R^2
Competitive Advantage	0.7983	0.7839
Frequency of Cyber Incidents	0.4185	0.4053
Regulatory Compliance	0.4646	0.4525

For **Competitive Advantage**, the adjusted R^2 value is 0.7839, indicating that the predictors explain 78.39% of the variance in this construct. This high value reflects the strong explanatory

power of the model in predicting **Competitive Advantage**.

In the case of **Frequency of Cyber Incidents**, the adjusted R^2 value is 0.4053, showing that 40.53% of the variance in this construct is explained by the independent variables. This suggests a moderate level of explanatory power.

Finally, for **Regulatory Compliance**, the adjusted R^2 value is 0.4525, meaning that 45.25% of the variance in **Regulatory Compliance** is accounted for by the model. This demonstrates a moderate level of explanatory power.

4.4 Overview of Effects and Inference Statistics

Table 9 presents an analysis of the relationships between constructs, highlighting the direct, indirect, and total effects alongside their statistical significance. In Figure 4, we can see a graphical representation of the model with the coefficients for the pathways theorized in this research.

The results indicate that **Cybersecurity Maturity** has a strong and statistically significant direct effect on **Competitive Advantage** ($\beta = 0.5547$, $t = 3.0449$, $p = 0.0023$). Additionally, **Cybersecurity Maturity** significantly influences **Frequency of Cyber Incidents** ($\beta = -0.6469$, $t = 8.5358$, $p < 0.0001$) and **Regulatory Compliance** ($\beta = 0.6816$, $t = 8.9747$, $p < 0.0001$), demonstrating robust effects.

The direct effect of **Regulatory Compliance** on **Competitive Advantage** is not significant ($\beta = 0.2374$, $t = 1.7491$, $p = 0.0803$). Furthermore, the direct effect of **Frequency of Cyber Incidents** on **Competitive Advantage** is also not statistically significant ($\beta = -0.2257$, $t = 1.5962$, $p = 0.1105$).

Furthermore, the indirect effect of **Cybersecurity Maturity** on **Competitive Advantage** through these mediators is not statistically significant ($\beta = 0.3078$, $t = 1.8614$, $p = 0.0627$). When considering both direct and indirect effects, the total effect of **Cybersecurity Maturity** on **Competitive Advantage** is strong and highly significant ($\beta = 0.8625$, $t = 26.3353$, $p < 0.0001$).

Table 9: Comprehensive Overview of Effects and Inference Statistics

Effect	Type	Direct Effect	Indirect Effect	Total Effect	t-value	p-value (2-sided)
Frequency Cyber Incidents → Competitive Advantage	Direct	-0.2257	–	–	1.5962	0.1105
Cybersecurity Maturity → Competitive Advantage	Direct	0.5547	–	–	3.0449	0.0023
Cybersecurity Maturity → Frequency Cyber Incidents	Direct	-0.6469	–	–	8.5358	0.0000
Cybersecurity Maturity → Regulatory Compliance	Direct	0.6816	–	–	8.9747	0.0000
Regulatory Compliance → Competitive Advantage	Direct	0.2374	–	–	1.7491	0.0803
Cybersecurity Maturity → Competitive Advantage	Indirect	–	0.3078	–	1.8614	0.0627
Frequency Cyber Incidents → Competitive Advantage	Total	–	–	-0.2257	1.5962	0.1105
Cybersecurity Maturity → Competitive Advantage	Total	–	–	0.8625	26.3353	0.0000
Cybersecurity Maturity → Frequency Cyber Incidents	Total	–	–	-0.6469	8.5358	0.0000
Cybersecurity Maturity → Regulatory Compliance	Total	–	–	0.6816	8.9747	0.0000
Regulatory Compliance → Competitive Advantage	Total	–	–	0.2374	1.7491	0.0803

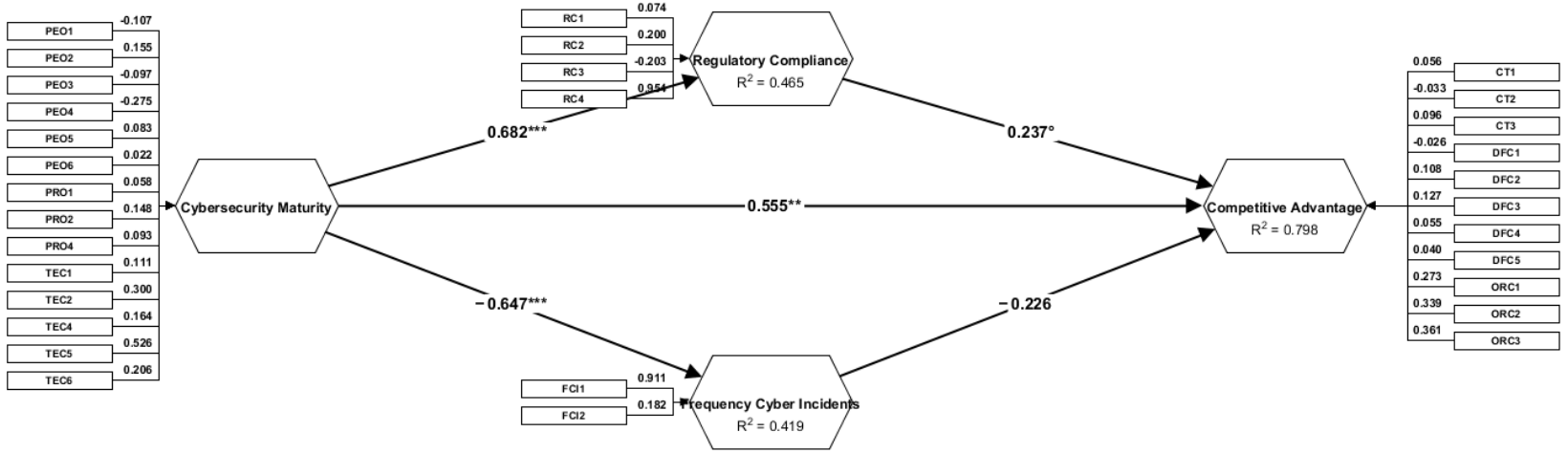

Figure 4: Representation of the Model in ADANCO

5 Discussion

The findings of this study highlight the strategic value of cybersecurity for SMEs, encouraging them to view it as an investment rather than a cost. Strengthening cybersecurity not only increases customer trust and enhances operational resilience but also differentiates SMEs from competitors. By proactively improving their cybersecurity posture, SMEs can gain a sustainable Competitive Advantage.

Despite the growing importance of cybersecurity, a notable gap exists in the literature; no quantitative evidence demonstrates Cybersecurity Maturity as a driver of Competitive Advantage for SMEs. To address this gap, this study adopts a quantitative approach tailored to SMEs, a group often overlooked in cybersecurity research, which primarily focuses on large organizations. By analysing key constructs such as Cybersecurity Maturity, Competitive Advantage, regulatory compliance, and the frequency of cyber incidents, this study provides empirical insights into how cybersecurity can serve as a strategic asset for SMEs.

5.1 Key Findings and Interpretations

The findings of this study reveal a strong and statistically significant direct effect of Cybersecurity Maturity on Competitive Advantage, reinforcing the notion that cybersecurity should not merely be a protective measure but that it should be a strategic asset for SMEs. However, the hypothesized mediating effects through regulatory compliance and the frequency of cyber incidents were not statistically significant. Despite these non-significant mediation effects, the model demonstrated an acceptable fit, supporting its validity in explaining the direct relationship between Cybersecurity Maturity and Competitive Advantage.

These results represent a novel contribution to the cybersecurity literature by providing empirical evidence of Cybersecurity Maturity as a driver of Competitive Advantage in SMEs, a topic that has been largely understudied in quantitative research. While prior studies have conceptually linked cybersecurity to business performance, this study is among the first to quantify this relationship, offering a data-driven validation of cybersecurity's strategic value for SMEs.

SMEs are often overlooked in cybersecurity research. By focussing on SMEs this study offers practical insights for decision-makers. The results highlight that investing in Cybersecurity Maturity can yield competitive benefits. This reframes cybersecurity investments from being perceived as a cost burden to a value-adding strategy, which is a critical shift in perspective for resource-constrained SMEs.

The findings of this research strongly support H1, as can be seen in Table 10 where the hypotheses of this study are repeated. The results align with the performed literature research suggesting that Cybersecurity Maturity is a driver of Competitive Advantage for SMEs. Previous research has stated that Cybersecurity Maturity enhances trust, operational resilience and continuity, and differentiation from competitors (Kosutic, 2021; Lloyd, 2020; Mmango & Gundu, 2024). This study substantiates this, demonstrating that SMEs with higher Cyberse-

Table 10: Summary of Hypotheses Testing Results

Hypothesis	Description	Hypothesis Status	Remarks
H1	Cybersecurity Maturity has a direct and positive effect on Competitive Advantage.	Supported	Strong statistically significant relationship supports the direct effect of Cybersecurity Maturity.
H2	Regulatory Compliance mediates the relationship between Cybersecurity Maturity and Competitive Advantage.	Not Supported	Lack of statistical significance suggests Regulatory Compliance does not mediate the relationship.
H3	Frequency of Cyber Incidents mediates the relationship between Cybersecurity Maturity and Competitive Advantage.	Not Supported	Results indicate no significant mediating effect for Frequency of Cyber Incidents.

curity Maturity are better equipped to build and maintain customer trust.

Moreover, the results support claims that robust cybersecurity practices contribute to minimizing operational disruptions, enabling SMEs to maintain business continuity (Al-Hawamleh, 2024; Altaha & Hafizur Rahman, 2023). This resilience can become a differentiating factor, particularly in competitive markets where customers and partners increasingly value security as a strategic asset. Thus, the positive relationship between Cybersecurity Maturity and Competitive Advantage found in this study show the importance of Cybersecurity Maturity as an enabler of Competitive Advantage for SMEs.

The results for H2 indicate that regulatory compliance does not mediate the relationship between Cybersecurity Maturity and Competitive Advantage, despite prior literature suggesting otherwise (Tikkinen-Piri et al., 2018; Vives, 2019). A possible explanation is that regulatory compliance is often perceived as a baseline requirement rather than a competitive differentiator. Unlike large corporations, SMEs may focus on meeting minimum compliance standards rather than leveraging them strategically to gain an advantage. Additionally, compliance efforts in SMEs are often reactive and resource-constrained, meaning they may not translate into broader business benefits beyond legal adherence. Future research could explore whether industry-specific regulatory demands or proactive compliance strategies influence this relationship.

Similarly, the results for H3 were not statistically significant, offering new perspectives on the relationship between cyber incident frequency and Competitive Advantage. While previous research suggests that reducing cyber incidents enhances trust and operational continuity (Bajwa et al., 2023; Dinkova et al., 2023), this study indicates that these benefits may not automatically translate into a competitive edge for SMEs. A possible explanation is that SMEs do not always effectively communicate their cybersecurity measures or incident reduction efforts to customers and stakeholders. This may limit their ability to differentiate based on security improvements. This highlights the need to explore the specific conditions under which cyber-

security improvements contribute to Competitive Advantage. Future research could focus on factors such as cybersecurity transparency, industry expectations, or customer perceptions.

However, the results did show that higher Cybersecurity Maturity leads to a reduced frequency of cyber incidents and enhanced regulatory compliance, both of which were statistically significant. These findings are consistent with the literature, which suggests that improved cybersecurity practices not only help mitigate cyber risks but also ensure compliance with industry regulations (Bajwa et al., 2023; Dinkova et al., 2023; Tikkinen-Piri et al., 2018). This underscores the foundational role of Cybersecurity Maturity in promoting operational stability and regulatory adherence, even if the previous mentioned factors did not mediate the relationship with Competitive Advantage in the present study.

5.2 Research Implications

This study contributes to the growing body of cybersecurity research, providing several important implications for both theory and practice, particularly in to what extent Cybersecurity Maturity can be leveraged to gain a Competitive Advantage for SMEs.

Firstly, the confirmation of a direct and positive relationship between Cybersecurity Maturity and Competitive Advantage reinforces the idea that cybersecurity should be viewed not only as a technical necessity but as a strategic asset for SMEs (Kosutic, 2021; Lloyd, 2020; Mmango & Gundu, 2024). This finding fills a gap in the existing literature by offering quantitative evidence of how Cybersecurity Maturity can provide SMEs with a competitive edge. Prior to this study, much of the research in this area focused on larger organizations, leaving SMEs without quantitative evidence on how cybersecurity investments contribute to their competitive advantage and long-term success. By providing quantitative evidence of the relationship between Cybersecurity Maturity and Competitive Advantage, this study helps bridge that gap and demonstrates how SMEs can strategically position cybersecurity as a differentiator in the marketplace.

Secondly, the non-significant results for the mediating roles of regulatory compliance and the frequency of cyber incidents suggest they may not translate Cybersecurity Maturity into Competitive Advantage for SMEs in the way that has been assumed in prior research. This highlights the complexity of how cybersecurity investments influence business performance and underscores the need for future studies to explore further the nuanced relationship between Cybersecurity Maturity and Competitive Advantage.

Lastly, the statistical significance of the relationships between Cybersecurity Maturity and, respectively, the frequency of cyber incidents and regulatory compliance suggests that investing in Cybersecurity Maturity can help SMEs reduce the chance of suffering from a successful cyber attack and enhance their regulatory standing. While these constructs did not directly mediate Competitive Advantage, they contribute to SMEs' foundational resilience and trustworthiness.

These implications are highly relevant for both SMEs and policymakers. For SMEs, the find-

ings provide a compelling case for investing in Cybersecurity Maturity, not just to safeguard their operations but also to gain a strategic advantage in an increasingly competitive digital marketplace. Cybersecurity should be viewed as a business enabler that can drive growth, build customer trust, and differentiate SMEs from their competitors. This study reframes cybersecurity investments from being a cost burden to an essential strategy for long-term success.

For policymakers and industry leaders, the study underscores the importance of initiatives that support SMEs in improving their cybersecurity posture. Governments and industry organizations should consider implementing targeted policies, such as subsidies and training programs, to help SMEs enhance their cybersecurity capabilities. These efforts will help protect SMEs from cyber threats and foster their long-term competitiveness and sustainability in the digital economy. By encouraging investments in cybersecurity, policymakers can help SMEs thrive in an increasingly complex and digital world, driving economic growth and innovation.

5.3 Limitations

While this research provides valuable insights into the relationship between Cybersecurity Maturity and Competitive Advantage, several limitations must be acknowledged. These limitations offer opportunities for future research and should be considered when interpreting the results.

First off, the methodology of the study relies on self-reported data collected through surveys. This may have introduced potential biases such as social desirability or response bias (Podsakoff et al., 2003). The responding SMEs may, for example, have overstated their organizations' Cybersecurity Maturity or compliance levels. Future research could address this limitation by using objective measures of Cybersecurity Maturity, such as cybersecurity audit results, to provide a more accurate representation of firms' cybersecurity capabilities.

Another limitation is the sample size and the potential for limited generalizability (Hair et al., 2022). Although the sample size that was reached in this research of 46 was sufficient for statistical analysis, a larger sample would have been preferred. The SMEs in the sample may not fully represent the broader population of SMEs. Different industry sectors, geographic locations, and organizational characteristics could result in varying levels of Cybersecurity Maturity and Competitive Advantage. Therefore, caution should be exercised when generalizing the results since these characteristics were not fully considered in this study. Future research could expand the sample to include a larger and more diverse range of SMEs, which could offer deeper insights into the varying effects of Cybersecurity Maturity across different contexts.

Finally, the absence of statistically significant mediation effects for regulatory compliance and the frequency of cyber incidents suggests that these factors may not directly contribute to Competitive Advantage for SMEs as previously assumed. This finding highlights the complexity of how cybersecurity investments translate into business performance and underscores the need for further research to refine the theoretical framework. Furthermore, the significant relationships between Cybersecurity Maturity and regulatory compliance and reduced frequency of cyber incidents indicate that these factors still play a crucial role in strengthening SMEs' resilience

and trustworthiness, even if they do not directly drive Competitive Advantage.

5.4 Future Research

Although this study has provided valuable insights into the relationship between Cybersecurity Maturity and Competitive Advantage for SMEs, several avenues for future research remain. Future research could use the findings and limitations discussed earlier to advance our understanding of Cybersecurity Maturity's role in creating and maintaining Competitive Advantage for SMEs.

One promising direction for future research is the exploration of the temporal relationships between Cybersecurity Maturity and Competitive Advantage. This study employed a cross-sectional design, which limits the ability to track effects through time. Future research could adopt a longitudinal approach to examine the evolution of the Cybersecurity Maturity of SMEs over time and assess how this evolution correlates with shifts in Competitive Advantage. A longitudinal study would offer a deeper understanding of the temporal dynamics between Cybersecurity Maturity and Competitive Advantage.

Additionally, the generalizability of the results could be expanded by including a more diverse range of SMEs in future research. This study gathered a relatively small sample, which may not fully represent the diversity of industries, geographic locations, or organizational sizes within the SME sector. A more diverse sample gathered through non-probability sampling would allow researchers to examine whether the relationship between Cybersecurity Maturity and Competitive Advantage varies across different contexts.

Finally, future research could investigate the individual impact of specific cybersecurity practices on Competitive Advantage. Cybersecurity Maturity is a broad construct; different aspects of cybersecurity, such as risk management and employee training, may have varying effects on Competitive Advantage. By disaggregating the components of Cybersecurity Maturity, future studies could provide more specific insights into which specific practices contribute most to Competitive Advantage, offering actionable recommendations for SMEs seeking to enhance their cybersecurity strategies.

6 Conclusion

Decision-makers in SMEs often struggle to allocate sufficient resources to cybersecurity, viewing it primarily as a defensive measure against cyber threats. However, this research challenges that perception by demonstrating that Cybersecurity Maturity is not just about protection but also a strategic enabler of Competitive Advantage. By adopting a quantitative approach, this study provides empirical evidence of a direct, statistically significant relationship between Cybersecurity Maturity and Competitive Advantage. These findings highlight a compelling business case for SMEs: those who proactively invest in cybersecurity differentiate themselves, build trust, and gain a competitive edge in an increasingly digital economy.

The results confirm that SMEs with higher Cybersecurity Maturity experience a direct and statistically significant improvement in their Competitive Advantage. This finding reinforces the growing recognition that cybersecurity is not merely a technical necessity but a means to build customer trust, improve operational resilience, and differentiate SMEs in the market. While the expected mediating effects of regulatory compliance and the frequency of cyber incidents were not statistically significant, this study still highlights the broader role of Cybersecurity Maturity in shaping SME competitiveness.

By addressing a key gap in cybersecurity research, the lack of quantitative evidence on cybersecurity's competitive benefits for SMEs, this study contributes both theoretically and practically. Theoretically, it expands the discussion on cybersecurity beyond risk mitigation to include its role in value creation and market positioning. Practically, the findings provide SMEs with a clear incentive to invest in cybersecurity not only to protect their assets but also to gain a sustainable Competitive Advantage.

Despite its valuable contributions, this study is not without limitations. The reliance on self-reported survey data may have introduced response biases, potentially affecting the accuracy of Cybersecurity Maturity assessments. Additionally, while the sample size was sufficient for statistical analysis, a larger and more diverse sample would enhance the generalizability of the findings. Future research should address these limitations by incorporating objective cybersecurity measures and by expanding the sample to include SMEs across various industries and regions. Despite these constraints, this study provides a strong foundation for understanding the strategic role of cybersecurity in SMEs, highlighting its potential as a key driver of Competitive Advantage.

The choice is clear: SMEs that fail to recognize cybersecurity's strategic value risk falling behind. SMEs that embrace cybersecurity are not just defending their businesses; they are building trust, strengthening resilience, and unlocking new market opportunities. This research shifts the cybersecurity conversation from cost to value, proving that proactive investment is not just necessary but highly rewarding. In our digital world, cybersecurity is no longer just a protective shield; it is a competitive weapon that ensures long-term success.

References

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*, 100031. https://doi.org/10.1016/j.csa.2023.100031

Ahmed, S. K. (2024). How to choose a sampling technique and determine sample size for research: A simplified guide for researchers. *Oral Oncology Reports*, *12*, 100662. https://doi.org/10.1016/j.oor.2024.100662

Alahmari, A. A., & Duncan, R. A. (2021). Investigating potential barriers to cybersecurity risk management investment in smes. *2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 1–6. https://doi.org/10.1109/ECAI52376.2021.9515166

Algan, N. (2019). The importance of smes on world economies. *Proceedings of International Conference on Eurasian Economies, Turkish Republic of Northern Cyprus*, *12*. https://doi.org/10.36880/C11.02265

Alharbi, F., Alsulami, M., AL-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., & Al-Otaibi, K. (2021). The Impact of Cybersecurity Practices on Cyberattack Damage: The Perspective of Small Enterprises in Saudi Arabia. *Sensors*, *21*(20). https://doi.org/10.3390/s21206901

Al-Hawamleh, A. (2024). Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. *International Journal of Computing and Digital Systems*, *15*(1), 1315–1331. https://doi.org/10.12785/ijcds/150193

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*, *305*, 357–383. https://doi.org/10.1016/j.ins.2015.01.025

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers Security*, *98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Altaha, S., & Hafizur Rahman, M. M. (2023). A mini literature review on integrating cybersecurity for business continuity. *2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, 353–359. https://doi.org/10.1109/ICAIIC57133.2023.10067127

Arroyabe, F. D. (2023). The severity and effects of cyber-breaches in smes: A machine learning approach. *Enterprise Information Systems*, *17*(3), 1942997. https://doi.org/10.1080/17517575.2021.1942997

Bajwa, I. A., Ahmad, S., Mahmud, M., & Bajwa, F. A. (2023). The impact of cyberattacks awareness on customers' trust and commitment: an empirical evidence from the Pakistani banking sector. *Information Computer Security*, *31*(5), 635–654. https://doi.org/10.1108/ICS-11-2022-0179

Barbier, J., Buckalew, L., Loucks, J., Moriarty, R., O'Connell, K., Riegel, M., & Cisco. (2016). *Cybersecurity as a Growth Advantage* (tech. rep.). https://www.cisco.com/c/dam/assets/offers/pdfs/cybersecurity-growth-advantage.pdf

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

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, *63*(4), 531–540. https://doi.org/10.1016/j.bushor.2020.03.010

Carias, J. F., Arrizabalaga, S., & Hernantes, J. (2021). Cyber Resilience Strategic Planning and Self-assessment Tool for Operationalization in SMEs BT - Information Technology in Disaster Risk Reduction. In Y. Murayama, D. Velev, & P. Zlateva (Eds.). Springer International Publishing. https://doi.org/10.1007/978-3-030-81469-4_21

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

Creswell, J. W. (2017, December). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications. https://www.ucg.ac.me/skladiste/blog_609332/objava_105202/fajlovi/Creswell.pdf

Dinkova, M., El-Dardiry, R., & Overvest, B. (2023). Should firms invest more in cybersecurity? *Small Business Economics*, *63*, 1–30. https://doi.org/10.1007/s11187-023-00803-0

Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. A. (2021). Software security patch management – a systematic literature review of challenges, approaches, tools and practices. https://arxiv.org/abs/2012.00544

EC, E. C. (2003). Commission recommendation of 6 may 2003 concerning the definition of micro, small and medium-sized enterprises (text with eea relevance) (notified under document number c(2003) 1422) [32003H0361]. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361

Eggers, F., O'Dwyer, M., Kraus, S., Vallaster, C., & Güldenberg, S. (2013). The impact of brand authenticity on brand trust and SME growth: A CEO perspective. *Journal of World Business*, *48*(3), 340–348. https://doi.org/10.1016/j.jwb.2012.07.018

El-Hajj, M., & Mirza, Z. (2024). ProtectingSmall and Medium Enterprises: A Specialized Cybersecurity Risk Assessment Framework and Tool. *Electronics*, *13*, 3910. https://doi.org/10.3390/electronics13193910

ENISA. (2021, June). *Cybersecurity for SMEs: Challenges and Recommendations.* (tech. rep.). https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

Etikan, I. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, *5*, 1. https://doi.org/10.11648/j.ajtas.20160501.11

EU. (2022, May). *SMEs and cybercrime* (tech. rep.). https://doi.org/doi:10.2837/14988

European Parliament & Council of the European Union. (2016, May 4). *Regulation (EU) 2016/679 of the European Parliament and of the Council* [Of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)]. Retrieved April 13, 2023, from https://data.europa.eu/eli/reg/2016/679/oj

European Union. (2022, December). The Network and Information 2 Directive - 2022/2555 - EN - EUR-LEX. http://data.europa.eu/eli/dir/2022/2555/oj

Gibb, A. A. (2000). Sme policy, academic research and the growth of ignorance, mythical concepts, myths, assumptions, rituals and confusions. *International Small Business Journal*, *18*(3), 13–35. https://doi.org/10.1177/0266242600183001

Golightly, L., Modesti, P., Garcia, R., & Chang, V. (2023). Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN. *Cyber Security and Applications*, *1*, 100015. https://doi.org/10.1016/j.csa.2023.100015

Hair, Black, W. C., Babin, B. J., & Anderson, R. E. (2009). *Multivariate data analysis*. Prentice Hall. https://www.drnishikantjha.com/papersCollection/Multivariate%20Data%20Analysis.pdf

Hair, Hult, T., Ringle, C., & Sarstedt, M. (2022, January). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. https://eli.johogo.com/Class/CCU/SEM/_A%20Primer%20on%20Partial%20Least%20Squares%20Structural%20Equation%20Modeling_Hair.pdf

Halikias, H. (2024). Preparation, Response, and Recovery. In *Digital shakedown: The complete guide to understanding and combating ransomware* (pp. 49–65). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-65438-1_4

Handri, E. Y., Putro, P. A. W., & Sensuse, D. I. (2023). Evaluating the people, process, and technology priorities for nist cybersecurity framework implementation in e-government. *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)*, 82–87. https://doi.org/10.1109/ICoCICs58778.2023.10277024

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

Hassan, A., & Ahmed, K. (2023). Cybersecurity's impact on customer experience: An analysis of data breaches and trust erosion. *Emerging Trends in Machine Intelligence and Big Data*, *15*(9), 1–19. https://orientreview.com/index.php/etmibd-journal/article/view/17

Henseler, J. (2017a). Bridging design and behavioral research with variance-based structural equation modeling. https://doi.org/10.1080/00913367.2017.1281780

Henseler, J. (2017b, February). *ADANCO 2.0.1 User Manual*. https://doi.org/10.13140/RG.2.2.30154.16321

Henson, R., & Sutcliffe, D. P. (2017). An insurance-based approach to improving sme cyber security. https://api.semanticscholar.org/CorpusID:56084349

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2021). Security Awareness: The First Step in Information Security Compliance Behavior. *Journal of Computer Information Systems*, *61*(4), 345–356. https://doi.org/10.1080/08874417.2019.1650676
doi: 10.1080/08874417.2019.1650676.

Islaqm, M. (2018). Sample size and its role in Central Limit Theorem (CLT). *4*, 1–7. https://doi.org/10.31295/ijpm.v1n1.42

Junior, C. R., Becker, I., & Johnson, S. (2023). Unaware, unfunded and uneducated: A systematic review of sme cybersecurity. https://arxiv.org/abs/2309.17186

Kante, M., & Michel, B. (2023). Use of partial least squares structural equation modelling (PLS-SEM) in privacy and disclosure research on social network sites: A systematic review. *Computers in Human Behavior Reports*, *10*, 100291. https://doi.org/10.1016/j.chbr.2023.100291

Keskin, O. F., Caramancion, K. M., Tatar, I., Raza, O., & Tatar, U. (2021). Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports. *Electronics*, *10*(10). https://doi.org/10.3390/electronics10101168

Kim, Y., Dykema, J., Stevenson, J., Black, P., & Moberg, D. P. (2018). Straightlining: Overview of Measurement, Comparison of Indicators, and Effects in Mail–Web Mixed-Mode Surveys. *Social Science Computer Review*, *37*(2), 214–233. https://doi.org/10.1177/0894439317752406

Kline, R. B. (2011, January). *Principles and practice of structural equation modeling, 3rd ed.* https://psycnet.apa.org/record/2010-18801-000

Koolen, C., Wuyts, K., Joosen, W., & Valcke, P. (2024). From insight to compliance: Appropriate technical and organisational security measures through the lens of cybersecurity maturity models. *Computer Law Security Review*, *52*, 105914. https://doi.org/10.1016/j.clsr.2023.105914

Kosutic, D. (2021, December). *The Impact of Cybersecurity on Competitive Advantage* [Doctoral dissertation]. https://www.researchgate.net/publication/357826918_The_Impact_of_Cybersecurity_on_Competitive_Advantage

Kwak, S. G., & Kim, J. H. (2017). Central limit theorem: the cornerstone of modern statistics. *Korean journal of anesthesiology*, *70*(2), 144–156. https://doi.org/10.4097/kjae.2017.70.2.144

Lakens, D. (2022). Sample size justification. *Collabra: Psychology*, *8*. https://doi.org/10.1525/collabra.33267

Lee, S. M., & Peterson, S. J. (2000). Culture, entrepreneurial orientation, and global competitiveness. *Journal of World Business*, *35*(4), 401–416. https://doi.org/10.1016/S1090-9516(00)00045-6

Lloyd, G. (2020). The business benefits of cyber security for SMEs. *Computer Fraud Security*, *2020*(2), 14–17. https://doi.org/10.1016/S1361-3723(20)30019-1

Lucas, J., & Harlee, M. (2024, December). *Innovative Cybersecurity Solutions for SMEs: Reducing Risks with Employee-Centric Awareness Programs*. https://doi.org/10.13140/RG.2.2.19660.12164

Meade, A. W., & Craig, S. B. (2012). Identifying careless responses in survey data. *Psychological methods*, *17 3*, 437–55. https://doi.org/10.1037/a0028085

Mmango, N., & Gundu, T. (2024). Cybersecurity as a Competitive Advantage for Entrepreneurs BT - South African Computer Science and Information Systems Research Trends. In A. Gerber (Ed.). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-64881-6_22

Otola, I., Grabowska, M., & Krupka, Z. (2023, November). *Trust and Organizational Resilience*. https://doi.org/10.4324/9781003433798

Patten, M. L., & Newhart, M. (2023, May). *Understanding research methods*. https://doi.org/10.4324/9781003092049

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. https://doi.org/10.1037/0021-9010.88.5.879

Ringle, C. M., Wende, S., & Becker, J.-M. (2024). Smartpls 4. https://www.smartpls.com/

Rohan, R., Funilkul, S., Pal, D., & Thapliyal, H. (2022). Humans in the loop: Cybersecurity aspects in the consumer iot context. *IEEE Consumer Electronics Magazine*, *11*(4), 78–84. https://doi.org/10.1109/MCE.2021.3095385

Saravanan, S., & Babu, C. V. (2024, April). Cybersecurity: Protecting information in a digital world. https://doi.org/10.4018/979-8-3693-0839-4.ch001

Sigalas, C. (2015). Competitive advantage: the known unknown concept. *Management Decision*, *53*, 2004–2016. https://doi.org/10.1108/MD-05-2015-0185

Sigalas, C., Pekka Economou, V., & B. Georgopoulos, N. (2013). Developing a measure of competitive advantage. *Journal of Strategy and Management*, *6*(4), 320–342. https://doi.org/10.1108/JSMA-03-2013-0015

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law Security Review*, *34*(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

Truong, T.-C., & Nguyen, H. K. (2024). Cybersecurity in Small and Medium-Sized Enterprises: A Bibliometric Analysis BT - From Smart City to Smart Factory for Sustainable Future: Conceptual Framework, Scenarios, and Multidiscipline Perspectives. In M. Pagac, J. Hajnys, T. Kozior, H.-S. Nguyen, V. D. Nguyen, & A. Nag (Eds.). Springer Nature Switzerland. https://repository.essex.ac.uk/38486/1/iSCSi%202023_PAPER%20ID%20188.pdf

Van Burg, E., Podoynitsyna, K., Beck, L., & Lommelen, T. (2012). Directive deficiencies: How resource constraints direct opportunity identification in smes. *Journal of Product Innovation Management*, *29*(6), 1000–1011. https://doi.org/10.1111/j.1540-5885.2012.00976.x

Vives, X. (2019). Digital Disruption in Banking. *Annual Review of Financial Economics*, *11*, 243–272. https://doi.org/10.1146/annurev-financial-100719-120854

Weston, R., & Faisal, A. (2024). Digital Technologies for SME Competitiveness: Unlocking the Power of AI and Cybersecurity. https://www.researchgate.net/publication/384443195_Digital_Technologies_for_SME_Competitiveness_Unlocking_the_Power_of_AI_and_Cybersecurity

Wilson, M., McDonald, S., Button, D., & McGarry, K. (2023). It Won't Happen to Me: Surveying SME Attitudes to Cyber-security. *Journal of Computer Information Systems*, *63*(2), 397–409. https://doi.org/10.1080/08874417.2022.2067791
doi: 10.1080/08874417.2022.2067791.

Yu, X., Zaza, I., Schuberth, F., & Henseler, J. (2021). Counterpoint: Representing forged concepts as emergent variables using composite-based structural equation modeling. *Data Base for Advances in Information Systems*, *52*(SI), 114–130. https://doi.org/10.1145/3505639.3505647

Zhang, C., & Conrad, F. G. (2014). Speeding in web surveys: The tendency to answer very fast and its association with straightlining. *Survey research methods*, *8*, 127–135. https://api.semanticscholar.org/CorpusID:59630570

Zott, C., & Amit, R. (2008). The Fit between Product Market Strategy and Business Model: Implications for Firm Performance. *Strategic Management Journal*, *29*(1), 1–26. http://www.jstor.org/stable/20141998

Appendix - The Survey

Survey Questions

Cybersecurity Pillars - People

Q1: Please indicate the extent to which you agree or disagree with the following statements regarding cybersecurity culture and awareness within your company.

Strongly disagree - Somewhat disagree - Neither agree nor disagree - Somewhat agree - Strongly agree

"Cybersecurity training and awareness are managed effectively in my company."
"Privileged users in my company understand their cybersecurity roles and responsibilities."
"My company has effective policies to protect private data."
"My company coordinates cybersecurity roles with internal and external partners."
"Cybersecurity awareness campaigns are conducted regularly in my company."
"Employees are encouraged to report any security incidents or concerns."

Cybersecurity Pillar - Process

Q2: Please indicate the extent to which you agree or disagree with the following statements about your company's approach to managing cybersecurity risks and preparing for incidents.

Strongly disagree - Somewhat disagree - Neither agree nor disagree - Somewhat agree - Strongly agree

"My company assesses cybersecurity risks when selecting external partners."
"Response and recovery plans are regularly tested and understood by personnel."
"Cybersecurity risks are integrated into our governance and risk management processes."
"My company identifies and manages cybersecurity risks in the supply chain."
"My company regularly reviews and updates incident response plans."

Cybersecurity Pillar - Technology

Q3: Please indicate the extent to which you agree or disagree with the following statements about your company's approach to managing cybersecurity risks and preparing for incidents.

Strongly disagree - Somewhat disagree - Neither agree nor disagree - Somewhat agree - Strongly agree

"Access to software and sensitive information is well managed in my company."

"Data leak prevention measures are in place in my company."
"Software and systems are updated and patched promptly in my company."
"Configuration and change control processes are followed in my company."
"We have real-time monitoring and response systems for cybersecurity threats."
"Backup systems are in place to ensure data recovery."

Frequency of Cyber Incidents

Q4: Please indicate the extent to which you agree or disagree with the following statements about the frequency of cyber incidents at your company.

Strongly disagree - Somewhat disagree - Neither agree nor disagree - Somewhat agree - Strongly agree

"Our cybersecurity policies and procedures have led to a reduction in the number of cybersecurity incidents."
"Our organization experiences fewer cyber incidents than our industry competitors."

Consumer Trust

Q5: Please indicate the extent to which you agree or disagree with the following statements about your company's customer loyalty and trust.

Strongly disagree - Somewhat disagree - Neither agree nor disagree - Somewhat agree - Strongly agree

"Our customers express high levels of satisfaction with our brand."
"Complaints about our products/services are rare."
"Customers frequently return for repeat purchases."
"Our customer base is loyal and consistently chooses us."

Differentiation from Competition

Q6: Please indicate the extent to which you agree or disagree with the following statements about how your company differentiates itself from competitors.

Strongly disagree - Somewhat disagree - Neither agree nor disagree - Somewhat agree - Strongly agree

"Our products/services are unique compared to competitors."
"We offer features or benefits that are hard for competitors to replicate."

"Our offerings are perceived as more innovative than competitors'."
"Our brand identity sets us apart from competitors."
"Our business is recognized for pioneering new ideas."

Operational Resilience and Continuity

Q7: Please indicate the extent to which you agree or disagree with the following statements regarding your company's preparedness for incident response and continuity of operations.

Strongly disagree - Somewhat disagree - Neither agree nor disagree - Somewhat agree - Strongly agree

"Employees know the steps needed to maintain critical assets during incidents."
"My company has documented recovery plans with time and point objectives."
"My business' continuity plans are regularly tested and updated."

Cybersecurity Regulation Compliance

Q8: Please indicate the extent to which you agree or disagree with the following statements regarding your company's compliance with cybersecurity regulations.

Strongly disagree - Somewhat disagree - Neither agree nor disagree - Somewhat agree - Strongly agree

"My company is aware of laws and regulations affecting our cybersecurity practices."
"My company has taken necessary actions to comply with GDPR."
"My company has taken actions to comply with the NIS2 Directive."
"My company has conducted compliance audits for cybersecurity regulations."