Nijmegen School of Management
Department of Economics and Business Economics
Masters Thesis Economics (MAN-MTHEC)

From awareness to action:

The role of cybersecurity awareness in investment behaviour among SME retailers

By Max Masselink (S1065064)

Nijmegen, 29 June 2025

Program: Master's Program in Economics
Specialisation: Financial Economics
Supervisor: R.H.R.M Aernoudts

Radboud Universiteit

ChatGPT, a Generative AI tool, is used to assist in coding, data analysis, and/or refining the language of this thesis. *Appendix 7.4* to this thesis provides a detailed account of the use of Generative AI tools during the development of this thesis. By submitting this thesis, I declare that I am fully responsible for the accuracy and completeness of its content.

Abstract

This study investigates the influence of cybersecurity awareness on the investment behaviour in cybersecurity measures of Dutch SME retailers. This research is relevant given the significant public investment in cybersecurity awareness campaigns. The study integrates the core constructs of Technology Acceptance Model, namely Perceived Usefulness (PU) and Perceived Ease of Use (PeoU), as a measure of cybersecurity awareness, with the NIST Framework as an instrument to measure investment level. The retail sector is becoming more dependent on digital infrastructure, making it important to understand the determinants of willingness to invest in cybersecurity measures.

Using a survey completed by SME retailers, this relationship was analysed through OLS regressions. The results show that PU and PEoU are positively related to the level of investment.

This study contributes to the literature by providing empirical evidence that awareness, when internalised as both useful and easy to apply, supports digital resilience in unregulated sectors such as retail. The study offers relevant and timely insight into the role of awareness as a strategic condition for cybersecurity resilience in SMEs. The findings support the hypothesis that cybersecurity awareness among SME retailers is positively associated with investment willingness.

Table of Contents

Introduction

1.1 Introduction to the research problem

Small and medium-sized enterprises (SMEs) play a significant role in the economy, but often face challenges in the field of cybersecurity. Despite increasing attention from policymakers, SMEs frequently lack the necessary resources and support to effectively manage cyber threats (van der Kleij, 2018). Chidukwani, Zander and Koutsakis (2022) note that cybersecurity research tends to focus on large enterprises, while studies involving SMEs are primarily qualitative, emphasizing risk assessment and preventive measures. Aspects such as detection, response, and recovery often remain underexplored. Within the broader SME landscape, the retail sector is of particular importance. The retail industry has undergone a digital transformation in recent years, resulting in greater dependence on information systems for their core business operations, customer interactions, and data management. This digitalization has increased the exposure of retail organisations to cyber risks (Vaka, 2025). In addition to its economic significance, as it creates value across the supply chain and provides entrepreneurial opportunities, the retail sector also faces notable vulnerabilities (Levy & Grewal, 2023). SME retailers exhibit limited cyber resilience and usually do not consider cybercrime as a substantial business risk. Nearly half of the companies surveyed had experienced a cyber incident in the preceding year, with 12% reporting financial or operational losses (Van der Kleij, De Bruin, Van 't Hoff-de Goede, Ancher, & Leukfeldt, 2019). This paper examines the influence of cybersecurity awareness on investments in cybersecurity measures within SMEs in the Netherlands, with a specific focus on companies in the retail sector.

Research by Thales (2022) indicates that 45% of retailers have experienced an increase in both the frequency and severity of cyberattacks. Additionally, 52% report a rise in incidents of e-commerce fraud (National Retail Federation, 2023). These developments point to an escalating threat landscape within a sector that is becoming increasingly dependent on digital infrastructure.

The integration of physical and digital sales channels has introduced new vulnerabilities. Organised Retail Crime no longer exclusively targets physical shoplifting but increasingly operates in digital environments using more advanced techniques (National Retail Federation, 2023).

Although awareness of cyber threats is increasing, many retailers appear to face difficulties in effectively responding to these risks. In many cases, cybersecurity approaches remain reactive rather than strategic, partly due to constrained resources and uncertainty regarding appropriate

countermeasures. This underscores the relevance of implementing both technical and organisational safeguards.

Given the interconnected nature of digital ecosystems, insufficient protection not only results in firm-level disruptions but may also lead to wider societal effects, including interruptions in critical processes and a decline in public trust in digital technologies (National Coordinator for Security and Counterterrorism, 2022; 2023).

1.2 Prior research

Heidt, Gerlach, & Buxmann (2019) examine the gap in IT security investments between small and medium-sized enterprises (SMEs) and large companies and argues that many existing IT security studies do not sufficiently consider the specific context of SMEs. Based on a literature review and interviews with 25 experts, the authors identified and validated SME-specific characteristics that affect IT security investments. The findings show that common assumptions in the literature, such as the presence of trained staff and documented processes, do not always apply to SMEs. While this study provides valuable insights into the structural challenges SMEs face in IT security investments, it does not specifically focus on the impact of cybersecurity awareness on investment decisions (Heidt, Gerlach, & Buxmann, 2019).

An ABN AMRO survey of 788 Dutch companies found that by 2024, around 20% of organizations had suffered damage because of a cyber-attack. The main consequences involved financial losses, loss of data and disruptions in business operations. Even though almost all companies surveyed say they have been victims of cybercrime at some point, confidence in their own cyber resilience remains remarkably high. SMEs emphasize preventive measures, while investments in detection, response and recovery often lag. This is worrying considering increasing threat complexity, including the rise of generative AI and geopolitically motivated attacks, which are currently only assessed as substantial by a limited proportion of companies (9%) (Koopal, 2025). A lack of awareness is seen here as the cause of the lagging innovations.

Although many SMEs consider cybersecurity important, in practice they often take insufficient action (Renaud & Ophoff, 2021). According to the authors, this is because companies do not always fully understand what the threat is, what actions are needed and why it is urgent to act. Factors such as misconceptions, too much information and a lack of time, money or knowledge are major obstacles in this regard. The study highlights the importance of clear, applicable support

and an understanding that cybersecurity is a shared responsibility within the organization (Renaud & Ophoff, 2021).

1.3 Theoretical relevance

Chidukwani, Zander, and Koutsakis (2022) identify a lack of research on detection, response, and recovery within SME cybersecurity and advocate for more quantitative studies in these areas. Little is known about the influence of cybersecurity awareness on investment decisions within SMEs. This is important as overall cybersecurity awareness appears to be insufficient (Al-Janabi, 2016). Technology alone is not sufficient to mitigate all security risks, given the complexity of the threat landscape. Therefore, it is important that users possess adequate awareness and skills to protect themselves effectively (Furnell & Clarke, 2012). The gap in cybersecurity awareness and investment behaviour is also reflected in empirical data: Statistics Netherlands (2024) reports that larger companies adopt cybersecurity measures more frequently than SMEs. Additionally, the National Coordinator for Security and Counterterrorism (2021) warns that SMEs often lack the expertise and financial resources to enhance their resilience, despite being attractive targets for cybercriminals. This study contributes to the literature by examining whether Dutch SMEs in the retail sector that are less aware of cybersecurity risks invest less in cybersecurity measures, and if such a relationship exists, what factors contribute to higher levels of cybersecurity awareness.

1.4 Practical relevance

This study provides empirical insight into the relationship between cybersecurity awareness and investment behaviour within SMEs. The results can support policymakers in evaluating the effectiveness of existing awareness campaigns and improving these initiatives to encourage more targeted security investments. In practice, it appears that many SMEs are insufficiently aware of the risks they are exposed to. ‘We see that cybercriminals are increasingly targeting SMEs because larger companies have their security in place better,’ said Richard Verbrugge, Information Security Risk Officer at ABN AMRO (2025). ‘Thus, a cyber-attack can affect not only companies, but also their suppliers and sometimes even the entire chain’ (Richard Verbrugge, 2025). This chain-wide vulnerability underlines the importance of awareness and preventive measures within SMEs. For this reason, the Dutch government has launched several initiatives aimed at strengthening the human factor in cyber defence, including awareness campaigns, podcasts, online tools and

webinars funded by public funds (Digital Government, 2025). Although these measures are designed to raise awareness, their actual impact on behavioural change and investment decisions remains unclear. It is therefore relevant to examine to what extent such campaigns lead SMEs to take concrete steps to improve their cybersecurity. More efficient use of public resources in this area can help increase societal resilience to cyber threats.

The NIS2 directive aims to strengthen the cybersecurity of organizations by imposing stricter requirements, expanding the scope of regulations, improving cooperation with Computer Security Incident Response Teams and promoting compliance with international standards (Ruohonemr, 2024). This team is responsible for detecting, analysing and coordinating responses to cybersecurity incidents within and across organizations. According to Netherlands Enterprise Agency (2025), only medium and large organizations in critical or very critical sectors are covered. As a result, SMEs in the retail sector are not legally required to implement cybersecurity measures. This absence of regulation provides a relevant context for this study to analyse the extent to which awareness campaigns and communication efforts, independent of legal obligations, contribute to investment readiness. The finding that awareness leads to action specifically when there is no legal pressure provides valuable input for the evaluation and development of policy measures.

1.5 Problem and research question

1.5.1 The systemic risk of cyber threats

"In cybersecurity, it is widely acknowledged that the resilience of one digital asset is contingent on the resilience of others, and the overall resilience of cyberspace depends on the security of its most vulnerable components" (Cobos, 2024, p. 80). When SMEs, which are often the most vulnerable links, are inadequately secured, this has a negative impact on the digital resilience of society. "Cyber risk is a textbook example of a systemic risk. Exposures to cyber risk are common across firms, and risks become highly correlated under stress" (Kopp, Wilson, & Kaffenberger, 2017, p. 7). This means the risks can spread and cause a wider impact, compromising the stability of the entire system. Systemic cyber risk refers to the risk that a cyber incident within one component of a critical infrastructure will lead to disruptions that spread to other components, potentially affecting service continuity, data integrity and economic, societal or national security (World Economic Forum, 2016). This reinforces the systemic nature of cyber risks, as vulnerabilities in one part of the supply chain can cascade throughout the entire network, affecting

multiple stakeholders. A security breach within the supply chain can have a direct impact on one's own organization. Suppliers can be a link in this, allowing malicious actors to gain access to critical systems of both the organization itself and its customers (National Cyber Security Centre, 2023).

1.5.2 Regulatory Context: The NIS2 Directive

The NIS2 Directive requires medium and large enterprises within critical sectors to implement enhanced cybersecurity measures, incident reporting and adherence to national strategies to promote cyber resilience. Member states are charged with monitoring compliance and imposing penalties for violations, while the European Union facilitates cooperation and information sharing to strengthen collective cybersecurity capabilities (European Commission, 2022). This NIS2 directive applies to many (critical and very critical) sectors, but not the retail sector (The Netherlands Enterprise Agency, 2025).

Only two in three large companies and less than half of SMEs are familiar with the NIS2 obligations; while many SMEs are not directly covered by the law, they do run the risk of having indirect obligations imposed on them through NIS2-compliant customers, while many larger companies are also not yet fully prepared for the law's entry into force in the third quarter of 2025 (Krauwer, 2025).

1.5.3 Research question and objectives

Since there is no specific legislation regarding cybersecurity for retail SMEs, cybersecurity is not always considered a primary objective. At the same time, the government makes substantial investments in awareness campaigns, funded with public resources, aimed at driving behavioural change among individuals and businesses because of the earlier mentioned systemic cyber risk. Previous research suggests that there are structural barriers within SMEs that hinder investment in cybersecurity. For instance, it appears that many assumptions about IT security, such as the availability of specialised staff and standardised processes, do not always apply to SMEs (Heidt, Gerlach, & Buxmann, 2019). In addition, a recent ABN AMRO survey of Dutch companies shows that confidence in their own cyber resilience remains high despite increasing damage from cyber-attacks and lagging investments in detection and recovery; a lack of awareness plays an important role in this (Koopal, 2025). Finally, previous work suggests that although cyber risk awareness among retail organisations is high, this does not automatically lead to implementation of effective security measures (Renaud & Ophoff, 2021). These findings underline that while there is

increasing attention to cyber security within SMEs, it is not yet known to what extent awareness leads to targeted investments in security measures, for this study specifically within the Dutch retail sector. Therefore, it is essential to examine:
Does the level of cybersecurity awareness affect investment in cybersecurity measures within small and medium-sized enterprises in the retail sector in the Netherlands?

1.6 Research design

A quantitative cross-sectional research design was chosen for this study to study the relationship between cybersecurity awareness and willingness to invest in cybersecurity measures among SME retail entrepreneurs in the Netherlands. A quantitative approach is appropriate because it allows statistical testing of relationships between awareness, perceptions and investment intention. A survey was conducted among SMEs in the Dutch retail sector, constructed based on the Technology Acceptance Model (TAM) (Davis, 1987), with Perceived Usefulness (PU) and Perceived Ease of Use (PEoU) being the central constructs for measuring awareness. The dependent variable, investment in cybersecurity, was measured using a composite index based on the NIST (National Institute of Standards and Technology, 2018) Cybersecurity Framework, which includes both technical and organizational measures (Almuhammadi & Alsaleh, 2017; Scofield, 2016). In addition, several control variables were included. This methodology provides a structured and replicable approach to analyse the extent to which awareness translates into concrete investment behaviour within an industry without direct regulatory pressure.

1.7 Structure of the study

The study follows a logical and orderly structure that leads to answering the central research question. *Chapter 2* provides the theoretical framework by reviewing literature on cybersecurity awareness, investment behaviour, and technology acceptance, and formulates the hypotheses for the empirical analysis. *Chapter 3* outlines the methodology, including research design, data collection, and variable operationalization. *Chapter 4* presents and interprets the regression results considering the hypotheses. *Chapter 5* summarizes the key findings, discusses theoretical and practical implications, addresses study limitations, and offers directions for future research.

2 Theoretical framework and hypotheses

The purpose of this chapter is to present the theoretical framework that supports this study and to formulate the central hypothesis based on relevant literature and conceptual models.

2.1 Cybersecurity awareness and implementation

Cybersecurity awareness is defined as "the knowledge and overall understanding of information-security-related problems and their repercussions as well as what needs to be done to handle them" (Khan, Ikram, & Saleem, 2023, p. 2). Building on the concept of cybersecurity awareness, organizations must translate this awareness into concrete actions, including strategic investments in cybersecurity, as well as the identification of critical assets and the implementation of organizational measures.

Cybersecurity investments in practice can consist of both technical and organizational measures. Technical investments include the implementation of firewalls, antivirus software, backup systems, and multi-factor authentication. Organizational investments involve the development of an information security policy, staff training, and the engagement of external expertise (Chidukwani, Zander, & Koutsakis, 2022; Jamil, Zia, Nayeem, Whitty, & Alessandro, 2025). This broad conceptualization aligns with previous studies that evaluate cybersecurity investments not based on exact financial expenditures, but on the number, variety, and degree of implementation of security measures (Rombaldo, Becker, & Johnson, 2023; Zwilling, Wiechetek, Lesjak, & Çetin, 2022). These studies emphasize the practical applicability and degree of integration of security practices within organizations.

These investments in IT security assets do not generate direct revenue but are primarily aimed at mitigating economic losses and opportunity costs by preventing and controlling cyber threats (Weishäupl, Yasasin, & Schryen, 2015).

The NIST Cybersecurity Framework (2018) offers an operationalisation of the broad approach to cybersecurity investments (Chidukwani, Zander, & Koutsakis, 2022; Rombaldo, Becker, & Johnson, 2023; Weishäupl, Yasasin, & Schryen, 2015). It aligns with scientific conceptualisations that define cybersecurity investments as a combination of technical and organisational measures, aimed at practical implementation and mitigation of economic risks within organisational contexts. The NIST Cybersecurity Framework offers a flexible, cross-sectoral structure that enables

organisations to identify, manage, and mitigate cyber risks through five core functions: Identify, Protect, Detect, Respond, and Recover. These are supported by implementation levels and framework profiles, that facilitate the assessment of maturity and prioritization of cybersecurity efforts. Jamil et al. (2025) emphasise the framework's relevance for small businesses. Their findings reveal that small businesses tend to score low across all NIST domains, reflecting a generally low level of cyber maturity. Moore et al. (2015) demonstrate that cybersecurity frameworks like NIST are widely adopted within organizations as tools for structuring investment decisions and aligning technical cybersecurity risks with broader business priorities. Building on these insights, their present study applies the NIST Framework to examine the extent to which Dutch SME retailers invest in cybersecurity measures.

Investments in cybersecurity contribute to the resilience of businesses; it is relevant to examine how such investments are implemented across different types of SMEs. In the Netherlands, SMEs are defined according to the criteria set out in Book 2 of the Dutch Civil Code and the European Accounting Directive (2013/34/EU), as amended by the Implementing Decree on the Increase of Thresholds (Ministry of Justice and Security, 2024). A company qualifies as a SME if it meets at least two of the following three criteria for two consecutive financial years:

- A balance sheet total not exceeding €25,000,000,
- A net turnover not exceeding €50,000,000,
- An average number of employees not exceeding 250.

2.2 The Information Security Awareness model

The Information Security Awareness (ISA) model of Haeussinger and Kranz (2013) provides an empirically based framework that explains how information security awareness is established and its role in explaining employees' intention to comply with security policies (Haeussinger & Kranz, 2013). Within this model, ISA is defined from a cognitive approach, as a state of awareness and knowledge about information security goals, risks and threats, and an interest in acquiring the necessary knowledge to act information responsibly (Haeussinger & Kranz, 2013). The authors identify several determinants of ISA, including knowledge about information systems and actively providing clear, understandable and available information security policies, as the most influential (Haeussinger & Kranz, 2013). In addition, they show that security training, information from secondary sources (such as media) and the behaviour of colleagues also contribute to the level of

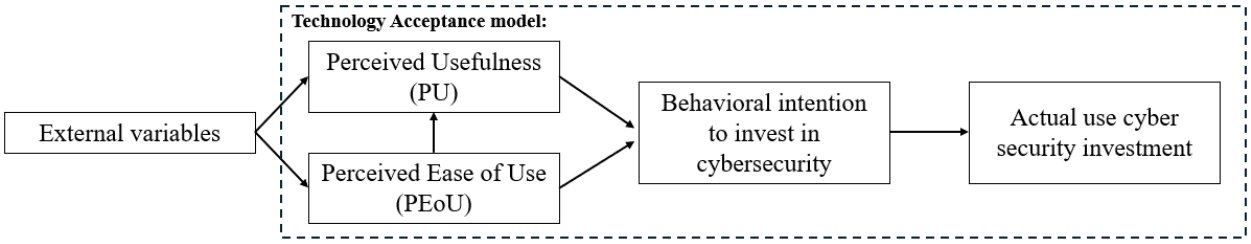
ISA (Haeussinger & Kranz, 2013). In their model is the role of ISA as a mediating variable: ISA mediates the relationship between these influencing factors and employees' intention to comply with security policies (Haeussinger & Kranz, 2013). In doing so, the authors find empirical evidence for a direct, positive relationship between ISA and compliance intention (Haeussinger & Kranz, 2013).

2.3 Cybersecurity training acceptance in SMEs

The acceptance of cybersecurity training has been studied using the Technology Acceptance Model (TAM) and its later extension, the Cybersecurity Training Acceptance Model (CTAM) (Fallatah, Kävrestad, & Furnell, 2024). The original TAM, developed by Davis (1987), explains technology acceptance through two constructs: perceived usefulness (PU) and perceived ease of use (PEoU). PU is defined as the extent to which a technology is perceived to enhance performance. In contrast, PEoU is defined as the perceived effort required to use it. Both constructs have been validated as strong predictors of behavioural intention (Holden & Karsh, 2010). In the context of cybersecurity, PU can be understood as the anticipated contribution of security measures to business continuity, whereas PEoU concerns how easily such measures can be implemented. Fallatah, Kävrestad & Furnell (2024) demonstrates that perceptions of threat and complexity influence both PU and PEoU, thereby shaping entrepreneurs' willingness to adopt cybersecurity tools.

Building on TAM, CTAM introduces additional contextual and psychological variables that influence participation in cybersecurity training among SMEs. These include regulatory control (perceived external pressure), worry (concern about cyber threats), apathy (indifference), and trust (confidence in available solutions) (Jamil, Zia, Nayeem, Whitty, & Alessandro, 2025). Other influential factors include perceived relevance, prior experience, management support, usability, social norms, self-efficacy, and enjoyment (Nurqamarani, Soegiarto, & Nurlaeli, 2021). Despite growing awareness, many SMEs still hesitate to act, often due to apathy or mistrust in the effectiveness of cybersecurity solutions. Fallatah, Kävrestad & Furnell (2024) highlights the need for a multifaceted training approach that clarifies benefits, increases choice, and fosters a supportive learning environment. These insights are relevant for retail SMEs, where awareness does not always lead to action. Understanding the cognitive and contextual factors behind this gap can help in designing more effective interventions to increase cybersecurity engagement.

Figure 1: Technology Acceptance Model



Note: Adapted from Sohn and Kwon (2020, p. 3)

To visually structure and theoretically substantiate the above insights, this study used the Technology Acceptance Model as elaborated by Sohn and Kwon (2020). They confirm that PU and PEoU are central determinants of behavioural intention and furthermore show that PEoU not only has a direct effect on behavioural intention, but also indirectly via PU. These insights from Sohn and Kwon (2020) have been translated to the context of cybersecurity training within Dutch SMEs, as shown in Figure 1. This adapted model shows how perceptions of threat and complexity influence willingness to implement cybersecurity measures indirectly via PU and PEoU. Thereby, the model provides a relevant theoretical capstone to better explain the gap between awareness and behaviour within retail SMEs.

2.4 Cybersecurity awareness and protective behaviour in SMEs

Cybersecurity awareness refers to the extent to which individuals within an organization recognize cyber threats, understand their potential impact, and are informed about measures to mitigate associated risks. Within the context of SMEs, this awareness is relevant, as such organizations often operate with limited resources and human behaviour can pose a vulnerability in the security framework (Furnell & Clarke, 2012; Jamil, Zia, Nayeem, Whitty, & Alessandro, 2025; White, 1980). Building on the understanding of cybersecurity training acceptance, it is important to examine whether cybersecurity awareness translates into concrete protective actions and investments within SMEs. A theoretical starting point of this research is the relationship between awareness, knowledge, and protective behaviour. Previous research shows that although internet users may be aware of cyber threats, this awareness does not necessarily lead to protective behaviour (Zwilling, Wiechetek, Lesjak, & Çetin, 2022). A comparative study conducted in Israel, Slovenia, Poland, and Turkey confirms that higher levels of cyber knowledge are associated with increased awareness and more frequent use of protective measures. However, this awareness does

not always translate into safer behaviour, as many individuals remain willing to share personal or sensitive information. This distinction between awareness and actual behaviour highlights that knowledge alone may not be sufficient. As Furnell and Clarke (2012) argue, effective protection requires not only technological solutions, but also usable systems and behavioural understanding, aligning with the concepts of PU and PEoU, to ensure that users are both able and willing to act securely. This view aligns with studies that assess cybersecurity awareness through self-reported data, typically focusing on three dimensions: knowledge, perceived threat, and behavioural intention (Shojaifar & Järvinen, 2021; Zwilling, Wiechetek, Lesjak, & Çetin, 2022). Additionally, Zwilling et al. (2022) note that awareness and protective behaviour vary by country, with higher levels observed in economically developed nations. In the Dutch context, the Cyber Security Raad (2024) highlights that limited cyber awareness and uncertainty around investments contribute to a heightened risk of cyber incidents among SMEs. This research builds on these insights by examining how cybersecurity awareness influences investment behaviour within Dutch SME retailers and whether sectoral differences can be identified.

2.5 Psychological drivers of cybersecurity investments

Cybersecurity awareness influences protective behaviour but does not automatically lead to more investment in cybersecurity measures. Protection Motivation Theory (PMT) explains protective behaviour through two cognitive processes: threat appraisal and coping appraisal. It identifies four relevant variables: threat severity, threat vulnerability, response efficacy and self-efficacy. (Rogers, 1975; Floyd, Prentice-Dunn, & Rogers, 2000). Jamil et al. (2025) applied this theoretical framework to a sample of micro-entrepreneurs in Australia and found that all four PMT components are predictors of cybersecurity-related behaviour. Their study also shows that high response costs, such as time investment or financial burden, negatively affect the willingness to invest in cybersecurity. These findings suggest that PMT offers a suitable framework for examining cybersecurity behaviour among SMEs, when perceptions of threat and the feasibility of protective actions are included in the analysis. Shojaifar and Järvinen (2021) confirm that self-efficacy and perceived severity have a positive influence on protective behaviour, while threat sensitivity has no effect, and stress the importance of targeted awareness campaigns for micro-entrepreneurs. SMEs can be divided into five categories based on cybersecurity competencies and awareness levels, which highlight the need for targeting strategies within the sector; in addition,

self-efficacy and organizational support, such as management encouragement, appear to be determinants of effective adoption of cybersecurity measures (Shojaifar & Järvinen, 2021).

2.6 Cybersecurity as a strategic business asset

The Resource-Based View (RBV) approaches cybersecurity investments as strategic business resources that contribute to long-term resilience and competitive advantage, distinguishing between tangible resources such as firewalls and intangible resources such as knowledge and training (Weishäupl, Yasasin, & Schryen, 2015). These investments do not generate immediate profits but mitigate potential losses and enhance organisational performance through interaction with other IT and business resources (Weishäupl, Yasasin, & Schryen, 2015). Some studies adopt a broader interpretation of investment behaviour by focusing not on exact expenditure, but on the quantity, variation and degree of implementation of security measures within organisations, with emphasis on practicality (Zwilling, Wiechetek, Lesjak, & Çetin, 2022). Madhani (2010) emphasises from the RBV that knowledge, skills and processes are strategic resources that, if deployed effectively, contribute to sustainable competitive advantage (Weishäupl, Yasasin, & Schryen, 2015).

2.7 Cyber threats and investment constraints within the SME retail sector

There has been an increase in successful cyber-attacks on SMEs, with a significant percentage of attacks specifically targeting them (Rombaldo, Becker, & Johnson, 2023). It has also been found that small businesses are not as aware of cybersecurity issues or as protected against them as they could be. This is mostly because they don't understand the risks well enough, don't invest enough, and don't know enough about cybersecurity. These factors highlight that cybersecurity awareness plays a role in making investment decisions within SMEs. A lack of awareness can cause companies to underestimate cyber threats and consider investments as unnecessary costs, while a higher level of awareness can encourage proactive security measures. Chidukwani, Zander and Koutsakis (2022) note that research on SME cyber security largely focuses on risk assessment and prevention, while the aspects of detection, response and recovery remain underexposed. This lack of a broad research base underlines the need to investigate how cybersecurity awareness among SMEs affects their investment behaviour. This research builds on this by specifically analysing the

extent to which cybersecurity awareness influences investments in security measures within Dutch SME retail companies (Chidukwani, Zander, & Koutsakis, 2022).

The lack of awareness of cyber threats is identified as a prominent and recurring theme, both as a motivation for research and finding in multiple studies. Moreover, the review suggests that limited cybersecurity literacy is an underlying cause of both low awareness and inadequate allocation of resources to cybersecurity, leaving SMEs vulnerable to cyber threats (Rombaldo, Becker, & Johnson, 2023).

This lack of cybersecurity awareness and limited resource allocation highlight the need for targeted measures to increase the cyber resilience of SMEs. Rick van der Kleij (2018) shows that specific interventions, such as improving IT knowledge and implementing a strict sanctions policy, can effectively contribute to increased protection against cyber threats. The cyber resilience of SME retailers can be improved by enhancing their ability to learn from cyber incidents (Van der Kleij, De Bruin, Van 't Hoff-de Goede, Ancher, & Leukfeldt, 2019). The study highlights that increasing employees' IT knowledge and implementing a strict sanctions policy for unsafe cyber behaviour are effective measures to improve overall cybersecurity readiness within SMEs. These findings are in line with the insights of Straub (1990), who examined how deterrence through sanctions and control can be an effective strategy to reduce misuse of IT systems.

Detmar Straub (1990) wrote that he examined the extent to which investment in information security contributes to the effective control of computer abuse, using General Deterrence Theory (GDT) as a theoretical framework. The theory states that sanctions act as deterrents, with both the certainty of sanction (the probability of being caught) and the severity of sanction (the severity of punishment) playing a role in deterring deviant behaviour. In the context of information security, deterrence is achieved through 'policing' activities, such as enforcing security policies, monitoring system usage and communicating sanctions for violations. The study confirms that tougher penalties and increased monitoring lead to less damage from intentional misuse and highlights the importance of both preventive software measures and deterrent policies in managing cyber threats. The results underline that cybersecurity is an effective strategy to reduce misuse within organizations and confirm the applicability of General Deterrence Theory in the cybersecurity context (Straub, 1990).

2.8 The role of legislation and impact on cybersecurity investments

Raising cybersecurity awareness and implementing preventive measures contribute to the resilience of SMEs, while the need for stricter regulation at the European level is becoming increasingly apparent. In this context, the European Union's NIS2 directive has been developed to strengthen the cybersecurity and resilience of services. The NIS2 directive, drafted by the European Union, aims to strengthen the cybersecurity and resilience of services within EU member states (European Commission, 2022).

The directive sets stricter obligations, such as a duty of care and duty of notification. Organizations must conduct risk assessments, implement appropriate security measures and report cyber incidents within 24 hours, under the supervision of independent authorities such as the National Digital Infrastructure Inspectorate (Digitale Overheid, 2019). However, it does not apply to SMEs in the retail sector (Government of the Netherlands, 2024).

2.9 TAM as an approach to cyber awareness

TAM provides a suitable framework to explain investment behaviour in cybersecurity because it predicts technology use based on PU and PEoU, two constructs that have been repeatedly validated as strong predictors of behavioural intention (Davis, 1987; Fallatah, Kävrestad, & Furnell, 2024). Unlike the contextualised CTAM, which focuses primarily on participation in cybersecurity training and adds multiple contextual factors, TAM remains theoretically simpler and more broadly applicable (Fallatah, Kävrestad, & Furnell, 2024). As such, TAM is better aligned with this research on individual investment readiness within retail SMEs.

PMT explains protective behaviour based on threat and coping perceptions such as self-efficacy and response-effectiveness (Rogers, 1975; Jamil, Zia, Nayeem, Whitty, & Alessandro, 2025), while TAM assumes rational trade-offs about the usability and ease of use of technology (Davis, 1987). Both models use similar concepts, such as the effectiveness of a measure, in PMT in the form of response effectiveness and in TAM as PU. Combining these models would create conceptual duplication, the same mechanism is then measured twice using different terms. This leads to multicollinearity in the analysis, where highly overlapping variables interfere with each others explanatory power. To avoid this kind of theoretical and statistical inconsistency, we chose to choose TAM as the main variable and PMT as the control variable in this study.

RBV considers cybersecurity measures as strategic business assets that contribute to long-term resilience and competitive advantage, but not necessarily to immediate behavioural intention (Weishäupl, Yasasin, & Schryen, 2015). Unlike TAM, which focuses on individual perceptions of utility and ease of use (Davis, 1987), RBV uses an organisational level with different assumptions about decision-making. Because of this theoretical mismatch and the focus of this study on individual investment willingness within SME retail, TAM is the most appropriate explanatory model. Therefore, we chose to choose TAM as the main variable and RBV as the control variable in this study.

2.10 Conceptual framework and hypotheses

Figure 2: Conceptual framework

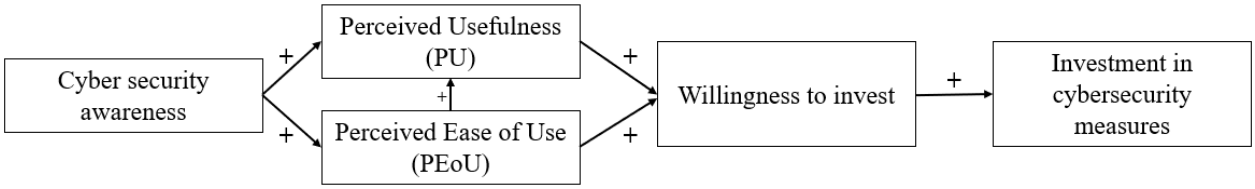


Figure 2 shows the conceptual model in which three successive steps explain the relationship between cybersecurity awareness and investment in cybersecurity measures among SME retailers.

The first step in the conceptual model progresses from cybersecurity awareness (ISA) to PU and PEoU. Based on Haeussinger & Kranz's (2013) model, knowledge about information systems and existing security measures contributes to increased information security awareness. This awareness then influences how entrepreneurs assess the usefulness (PU) and feasibility (PEoU) of cybersecurity measures (Haeussinger & Kranz, 2013; Davis, 1987). Without awareness, security solutions are often overlooked or perceived as unnecessarily complicated.

The second step follows the TAM, in which PU and PEoU together predict behavioural intention (Fallatah, Kävrestad, & Furnell, 2024). Entrepreneurs who perceive measures as useful and user-friendly are more likely to invest. Research also shows that PEoU has a reinforcing effect on PU: the simpler a measure seems, the more useful it is perceived to be (Sohn & Kwon, 2019). PU and PEoU thus form the core of investment readiness in cybersecurity.

The third step concerns the transition from willingness to actual investment in cybersecurity measures. Entrepreneurs who are willing to invest are more likely to convert this intention into concrete actions, such as implementing technical or organisational security measures. This is

confirmed by Jamil et al (2025), who show that higher investment intention is strongly correlated with actual cybersecurity behaviour.

Therefore, the hypothesis of this study is formulated as follows:

H1: Ceteris paribus, an increase in cybersecurity awareness among SME retailers leads to a greater willingness to invest in cybersecurity measures.

3 Methodology

The purpose of this chapter is to outline the methodological approach of the study, including the research design, data collection process, and the operationalisation of key variables.

3.1 Research design

3.1.1 Methodological approach

This study employs a quantitative, cross-sectional survey design to examine the relationship between cybersecurity awareness and investment in cybersecurity measures among Dutch SME retailers. A cross-sectional approach was selected due to limited time and resources to conduct longitudinal measurements. The survey method was chosen because it enables targeted data collection on cybersecurity investments and awareness within a specific population for which such data are generally not publicly available. Publicly accessible information on cybersecurity in SMEs remains limited (Chidukwani, Zander, & Koutsakis, 2022; Rombaldo, Becker, & Johnson, 2023). Participation in this study is voluntary. Data were collected using a web-based survey administered through Qualtrics. This study uses 7-point Likert-type scales to measure PU, PEoU and NIST. Likert scales were chosen for their simplicity and effectiveness in measuring degrees of perceptions and attitudes (Davis, 1987). These scales are widely accepted and often used in social science research because they can accurately and repeatably measure the intensity of feelings, attitudes and beliefs (Davis, 1987). The survey was conducted in Dutch to ensure the comprehensibility and accuracy of the answers, as the target group consisted exclusively of Dutch SME entrepreneurs. To encourage participation, a gift card raffle was held among all respondents who completed the survey. The incentive was announced in the recruitment message, and participation remained voluntary and anonymous throughout.

3.2 Data

3.2.1 Descriptive and summarize statistics

Table 1: Descriptive statistics.

Variable	Full variable	Measurement
PU	Perceived Usefulness.	Likert scale (1-8)
PEoU	Perceived Ease of Use.	Likert scale (1-8)
NIST	National Institute of Standards and Technology.	Likert scale (1-8)
PMT	Measured using items reflecting perceived threat, vulnerability, and response efficacy based on Protection Motivation Theory.	Likert scale (1-8)
RBV	Measured through agreement with statements on the uniqueness and strategic value of internal cybersecurity resources and capabilities.	Likert scale (1-8)
Age	Measured as the respondent's age in years.	Categorical
Gender	Measure the gender of the respondent, with answer options male or female.	Dummy (1=men, 2 = women)
IT-Responsible	Measured by asking who is responsible for IT or cybersecurity within the organization (internal, external, both, or no one).	Categorical
Systems	Measured through a categorical item assessing whether digital systems are used for core business activities.	Categorical
Province	Measured as a multiple-choice categorical variable indicating the province(s) where the business is located, more options possible.	Categorical

The Likert scale statements were answered on a scale of 1 to 7, with 1 representing 'totally disagree' and 7 representing 'totally agree'. Option 8 stood for 'don't know / no opinion' and was treated as a separate category or excluded in the analysis, depending on the analysis.

Table 2 is a schematic representation of the variable used in this paper. This shows the number of observations, mean, standard error, minimum and maximum.

Table 2: Summarize statistics.

Variable	Obs	Mean	Std. dev.	Min	Max
PU	41	5.439	0.821	2.938	7.000
PEoU	41	4.791	0.755	2.062	6.615
NIST	40	5.793	0.651	4.273	6.727

Table 3: Responses

	Obs
Total responses	103
Retail	80
SME	52
Only foreign	0
Target group	41

Table 4: Summarize statistics.

Variable	Obs	Mean	Std. dev.	Min	Max
PU	40	5.400	0.792	2.938	6.562
PEoU	40	4.745	0.705	2.062	5.875
NIST	40	5.793	0.651	4.273	6.727

Table 3 shows the extent to which survey respondents meet the criteria to be included in the research population of this study. The target population of the survey consists of respondents who are active in the retail sector, who meet the criteria for an SME in two consecutive years and who are based in the Netherlands. A total of 41 respondents met these selection criteria.

The NIST score in *table 2* contains one less observation than the other variables because one respondent chose the response option ‘Don't know / no opinion’ for all items in this scale. These responses are coded in the dataset as missing values (NA) and are therefore excluded from the analysis.

Of the 41 respondents, the above respondent was excluded in the calculation of the NIST score, bringing the number of usable observations for this variable to 40. This exclusion helps to clean up the dataset, as the data show that this respondent often consistently chose the rightmost answer option. This led to a maximum score of 7 at the PU scale (*table 3*), which after exclusion also decreased to 6,562 (*table 4*), indicating a less biased picture of the mean responses.

3.2.2 Bootstrapping PU and PEoU

There were only 40 usable responses for this study. Given that this is a small sample size, bootstrapping was applied as an additional method to test the robustness of the regression results. Bootstrapping is a statistical technique in which random samples with replacement are repeatedly drawn from the original dataset, allowing evaluation of whether the observed effects are stable and consistent. In this analysis, the bootstrap was limited to the core variables PU and PEoU. Attempts to bootstrap the full model including control variables proved unfeasible, as some categorical variables were insufficiently represented in many resampled datasets. This led to error messages or non-converging regressions. Therefore, it was decided to apply the bootstrap analysis only to the simplified model with PU and PEoU as predictors of investment in cybersecurity measures. A total of 10,000 iterations were performed to minimize the impact of random variation (Monte Carlo variation) and obtain reliable confidence intervals (Hesterberg, 2011). This approach provides a robust and realistic estimation of the reliability of the relationships in the base model.

3.2.3 Cronbach's alpha

Cronbach's alpha is a commonly used measure of the internal consistency and reliability of a scale, which assumes that the items measure the same underlying construct (Tavakol & Dennick, 2011). The reliability of the scales in this study ranges from acceptable to excellent: the alpha for PU is very high ($\alpha = 0.893$), as is that for PeoU ($\alpha = 0.814$), indicating good internal consistency. The scale for NIST shows acceptable reliability with $\alpha = 0.728$. These results indicate that the measurement scales used in this study are sufficiently reliable for further analysis.

3.2.4 Dependent variable

The dependent variable in this study is the level of investment in cybersecurity measures among Dutch SME retailers. This variable is measured using a composite index score derived from survey questions designed to assess the extent to which organizations have implemented specific cybersecurity practices. The formulation of these questions is based on the NIST Cybersecurity Framework, which includes five core functions (Identify, Protect, Detect, Respond, Recover) and 23 categories (Almuhammadi & Alsaleh, 2017; Scofield, 2016). These 23 categories will be used to construct the survey questions. Jamil et al. (2025) also refer to the NIST Framework as a useful structure for evaluating cybersecurity practices within small enterprises. Each survey item is linked to one or more subcategories, thereby capturing the presence of security measures. Respondents

indicate the extent to which each statement applies to them or their organization, using a Likert scale. These responses are used to construct a continuous index score that captures both the breadth and depth of cybersecurity practices. This method allows for a quantitative comparison of cybersecurity investment levels across respondents and aligns with previous empirical studies (Moore, Dynes, & Chang, 2015; Jamil, Zia, Nayeem, Whitty, & Alessandro, 2025).

3.2.5 Independent variable

The independent variable in this study is cybersecurity awareness, defined as "the knowledge and overall understanding of information-security-related problems and their repercussions as well as what needs to be done to handle them" (Khan, Ikram, & Saleem, 2023, p. 2). The survey questions are based on the TAM. This model emphasizes factors such as PU and PEoU (Davis, 1987; Fallatah, Kävrestad, & Furnell, 2024). PU and PeOU were each surveyed in their own section of the survey through 16 Likert scale statements each. Respondents indicate the extent to which each statement applies to their organization using a 7-point Likert scale. Based on their responses, a score is calculated to reflect their level of cybersecurity awareness. This method enables a quantitative comparison of awareness levels across respondents and aligns with previous research in which cybersecurity is regarded not only as a technical issue but also as a strategic and psychological factor (Fallatah, Kävrestad, & Furnell, 2024).

3.2.6 Control variable

3.2.6.1 Demographic variables

Regional characteristics may affect digital processes, as the impact of digital infrastructure on socio-economic outcomes differs significantly between regions with different levels of development, justifying the inclusion of geographical factors as a control variable in research on digital development (Duanmu, Yuan, Zhang, & Yu, 2025). Therefore, this study includes the effect of regional differences within the Netherlands as a control variable. Respondents indicate the province in which their company is located so that it can be examined whether geographical factors are related to differences in willingness to invest in cybersecurity.

3.2.6.2 Gender

Gender is included as a control variable to analyse whether there are differences in willingness to invest in cybersecurity between male and female respondents. Respondents indicate their gender in the survey, which allows controlling for possible effects of gender on decision-making around digital security. Gender influences cybersecurity behaviour, as men and women differ significantly in self-reported behaviour, previous experience and security self-efficacy, justifying the inclusion of gender as a control variable in cybersecurity research (Anwar, He, Ash, Yuan, & Li, 2017).

3.2.6.3 Age

Age is included as a control variable because older and younger entrepreneurs may differ in their knowledge, experience or attitude towards cybersecurity measures. By asking respondents age in the survey, it is possible to examine whether age is related to differences in investment readiness. Age influences the cybersecurity awareness of decision makers, as respondents who were aware of certain threats and solutions were significantly older than those who were unaware of them, justifying the inclusion of age as a control variable in cybersecurity research (Vrhovec & Markelj, 2024).

3.2.6.4 Use of digital systems

To include differences in the use of digital technologies between firms in the analysis, the survey asks whether the organization uses digital systems for core activities, such as inventory management, customer communications or payments. This control variable provides insight into the extent to which companies work digitally. Organizations that make more intensive use of digital systems, may be more dependent on digital processes and therefore more likely to invest in cybersecurity measures. The degree of use of digital systems is included as a control variable, as digital transformation leads to higher cyber risks and thus increases the need for security investments (Saeed, Altamimi, Alkayyal, Alshehri, & Alabbad, 2023). This makes it possible to test whether companies that operate more digitally are also more willing to invest in cybersecurity than traditional retailers.

3.2.6.5 Availability of IT or cybersecurity officer

The availability of an IT or cybersecurity officer is included as a control variable in this study, as it may influence willingness to invest in digital security. Respondents indicate whether their organization has an employee or external party responsible for IT or cybersecurity. This control variable makes it possible to analyse whether the presence of internal and/or external specialized support is associated with a greater willingness to invest. The paper substantiates the relevance of including this variable by showing that the lack of specialized support within SMEs leads to limited expertise, conflicting responsibilities and lower priority for security, thus representing a significant barrier to effective cybersecurity and investment readiness (Rombaldo, Becker, & Johnson, 2023).

3.2.6.6 Sales and communication channels

The organization’s primary sales and communication channel is included as a control variable, with respondents indicating through which channels their company primarily engages in customer contact and/or sales. This will help determine whether channel choice influences investment decisions related to cybersecurity. E-commerce businesses operating through digital systems and online sales and communication channels are constantly exposed to serious cyber threats, requiring significant and continuous investments in security (Liu, et al., 2022). This justifies including both the use of digital systems and channel choice as control variables in research on cybersecurity expenditures.

3.2.6.7 Theoretical control models: PMT & RBV

In addition to contextual variables, insights from existing theories are also involved in the analysis. PMT states that perceptions of threat, vulnerability and effectiveness of measures can influence behaviour (Floyd, Prentice-Dunn, & Rogers, 2000). These are included to check the extent to which these perceptions are related to investment propensity. RBV is applied, which states that organizations are more likely to invest in cybersecurity when they see it as strategically valuable (Weishäupl, Yasasin, & Schryen, 2015). The survey therefore includes statements about the strategic value of cybersecurity and the presence of required resources. The inclusion of these elements makes it possible to control for the influence of underlying beliefs on investment behaviour.

3.3 Estimation

To estimate the relationship between cybersecurity awareness and the level of investment in cybersecurity measures among Dutch SME retailers, this study applies an Ordinary Least Squares (OLS) regression model. Cross-sectional data is used, which is constructed from survey responses collected via an online questionnaire. The choice for OLS is appropriate given the continuous nature of the dependent variable; namely, an index measuring the implementation of cybersecurity measures based on the NIST Cybersecurity Framework.

The regression equation is specified as follows:

$$(1) \qquad Y_i = \beta_{0,} + \beta_1 Awareness_i + \beta_2 X_i + \epsilon_{it}$$

In this study, Y_i denotes the level of investment in cybersecurity measures by firm i, measured using a composite index score based on the NIST Cybersecurity Framework. Awareness_i represents the cybersecurity awareness score of firm i, operationalized as the arithmetic mean of two core constructs from TAM: PU and PEoU. This measure reflects the perceived value and ease of engaging with cybersecurity-related tools and training. X_i is a vector of control variables, including age, gender, digital maturity, the presence of an IT specialist, regional location, and additional theoretical constructs such as PMT and RBV. Finally, ε_i is the error term capturing the unexplained variance in the level of investment.

The model aims to capture the general relationship between cybersecurity awareness and investment behaviour within the specific context of the Dutch SME retail sector. As the data are cross-sectional and gathered at a single point in time, no fixed effects or time trends are included. To address potential heteroskedasticity and ensure the reliability of inference, robust standard errors are estimated following the method proposed by White (1980). This accounts for possible differences in variance across observations, relevant given the heterogeneity among SMEs. The coefficient β_1 is expected to be positive, consistent with hypothesis 1, which states that higher levels of awareness lead to greater investment in cybersecurity measures.

4 Results

This chapter presents the empirical results, including regression outcomes and robustness checks. It covers the effects of PU, PEoU, and their interaction on cybersecurity investment, and reports on control variables and a bootstrap analysis for estimate stability.

4.1 Multicollinearity tests

Table 5 shows the correlations between all explanatory variables in the context of a multicollinearity analysis. Most variables correlate only weakly to moderately with each other, indicating limited overlap in explanatory power. The highest correlation is visible between PU and PMT (r = 0.73), indicating a strong correlation. This is consistent with the previously mentioned motivation for choosing TAM in *section 2.9* because combining these models would create conceptual duplication. The correlation between PU and PEoU (r = 0.55) can also be explained and is consistent with the conceptual model (Figure 2), which assumes that PEoU has a reinforcing effect on PU: the simpler a measure is perceived to be, the more useful it is rated (Sohn & Kwon, 2019). The correlation between PEoU and Systems (r = 0.41) are also significant but are also within acceptable limits. Notable are the negative correlations between Gender and PU (r = -0.28) and between Gender and PEoU (r = -0.50), indicating opposite patterns based on gender.

Table 5: Multicollinearity test.

	PU	PEoU	PMT	RBV	Age	Gender	IT-responsible	Systems	Province
PU	1								
PEoU	0.55	1							
PMT	0.73	0.54	1						
RBV	0.19	-0.02	0.39	1					
Age	0.10	0.01	0.10	0.07	1				
Gender	-0.28	-0.50	-0.38	-0.03	0.28	1			
IT-responsible	0.24	0.36	0.21	-0.05	0.03	-0.09	1		
Systems	0.24	0.41	0.32	0.26	0.00	-0.16	0.05	1	
Province	0.28	0.25	0.20	-0.03	-0.12	-0.10	0.01	0.28	1

Table 6 shows the results of the Variance Inflation Factor (VIF) test, which is used to detect possible multicollinearity between the independent variables. A VIF value below 5 is generally considered acceptable and usually does not indicate severe multicollinearity. In this case, the mean VIF is 1.72, which is relatively low and suggests that there is no problematic interdependence between the explanatory variables. PU (2.23), PEoU (2.34) and PMT (2.79) have the highest values, but remain well below the critical limit. It makes sense that these values are higher, given their theoretical consistency. PU and PEoU are both core constructs within the same model (TAM) where the multicollinearity is in line with the conceptual model *(figure 2)* and the given theories (Sohn & Kwon, 2019). PMT overlaps substantively with TAM. This VIF score (2.79) confirms the choice to keep PMT out of the main model and only include it as a control variable.

This does not mean that the variables are irrelevant; it merely indicates that their explanatory power is partly shared. The remaining variables, such as age, gender and IT responsibility, show VIF values close to 1, confirming the absence of confounding correlation. Based on this test, multicollinearity does not compromise the reliability of the regression results.

Table 6: VIF-test.

Variable	VIF	1/VIF
PU	2.23	0.45
PEoU	2.34	0.43
PMT	2.79	0.36
RBV	1.47	0.68
Age	1.18	0.85
Gender	1.62	0.62
IT-responsible	1.15	0.87
Systems	1.46	0.68
Province	1.20	0.83
Mean VIF	1.72	0.64

4.2 Regressions

4.2.1 OLS models: PU and PEoU on cybersecurity investment

Table 7 examines the influence of PU and PEoU on investment in cybersecurity, operationalized using the NIST score. In model (1), PU is included as the only explanatory variable. The coefficient is positive and statistically significant ($\beta = 0.377$, $p < 0.001$), with a low standard error (0.118), indicating a reliable estimate. This suggests that higher perceived usability is associated with an increase in cybersecurity investment.

In model (2), only PEoU is included. Again, the coefficient is positive and significant ($\beta = 0.411$, $p < 0.001$), with a slightly higher standard error (0.134), but still within acceptable limits. This suggests that the perceived user-friendliness of cybersecurity measures also plays a relevant role in investment behaviour.

Model (3) contains both PU and PEoU simultaneously. Although both coefficients remain positive (PU = 0.260; PEoU = 0.268), neither is statistically significant, and the standard errors increase (0.132 and 0.148, respectively). A likely explanation for this is multicollinearity: PU and PEoU are conceptually related and empirically correlated (Sohn & Kwon, 2019) , which can lead to overlapping explained variance. This decreases the precision of the individual estimates, and hence their statistical significance. However, the explanatory power of the combined model remains intact.

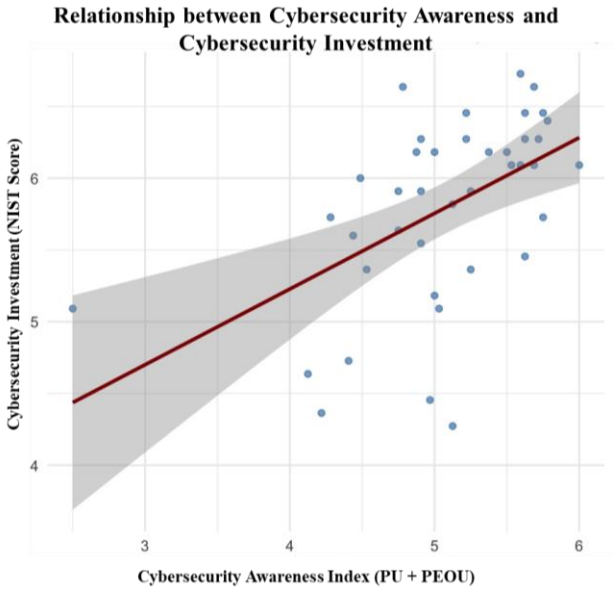
The explained variance (R^2) increases from 0.210 in model (1) and 0.198 in model (2) to 0.274 in model (3). The increase in adjusted R^2 from 0.189 to 0.235 supports the conclusion that the combined model is better able to explain variation in investment. Although the individual effects do not emerge as strongly, model (3) shows a more robust joint relationship between the explanatory variables and the level of investment.

Table 7: PU and PEoU on NIST

	Dependent variable:		
	Cybersecurity Investment (NIST)		
	PU only	PEoU only	PU + PEoU
	(1)	(2)	(3)
PU	0.377**		0.260
	(0.118)		(0.132)
PEoU		0.411**	0.268
		(0.134)	(0.148)
Constant	3.760***	3.843***	3.118***
	(0.646)	(0.643)	(0.721)
Observations	40	40	40
R^2	0.210	0.198	0.274
Adjusted R^2	0.189	0.177	0.235
Note:	*p**p***p<0.001		
	* p<0.001		

Figure 3 shows the relationship between PU + PEoU and NIST. This visualisation is consistent with the regression results in Table 7, which indicate a positive effect of awareness on investment level. The regression line in the graph shows a clear rising line, indicating a positive linear relationship between awareness and investment, consistent with the significance and direction of the coefficients in the regression model. Notable is one respondent on the x-axis, who scores relatively high on investment despite a very low awareness score. Since this observation might affect the regression line, an additional robustness check was performed using Cook's Distance. Cook's Distance is a measure to determine how much influence an individual observation has on the estimated coefficients in a linear regression. This influence is measured by comparing the regression model with and without that observation, where large values may indicate an influential or outlier observation (Cook, 2011, p. 301). The analysis showed that eight observations including this outlier were above the threshold value of 4/n and thus can be considered relatively influential. This suggests that some data points have above-average weight in the regression model. However, as the sample size in this study is limited (n = 40), we chose not to exclude these observations but report the possible influence in the *"Limitations and Future Research"* section. The corresponding graph and the results of the Cook's Distance analysis are included in *Appendix 7.2*.

Figure 3: Cook's Distance-analyse



4.2.2 Bootstrap confidence intervals

Table 8 shows the results of a bootstrap analysis for PU and PEoU, designed to test the robustness of their estimated effects on investment intention in cybersecurity. For PU, the mean coefficient is 0.272 (SD = 0.150), with a 95% confidence interval of -0.036 to 0.552. For PEoU, the mean is 0.293 (SD = 0.167), with an interval of -0.016 to 0.647. Although both variables indicate a positive impact, the confidence intervals span zero. This means that the effects are not statistically significant, and no firm conclusions can be drawn about the individual effect of PU or PEoU on investment behaviour based on these bootstrap results.

One possible explanation for the lack of significance is the limited sample size, combined with overlapping explanatory power of PU and PEoU. These constructs are conceptually related and empirically correlated, which may result in their separate effects being difficult to distinguish. In bootstrap analyses, confidence intervals are often estimated more conservatively or broadly, especially when the sample is small. As a result, those intervals more often fall over the number zero, meaning that an effect is statistically considered "not significant", even if the data do indicate an association. The direction and size of the coefficients suggest that PU and PEoU may both contribute to investment propensity, although additional research with larger samples is needed to establish this with certainty.

Table 8: Bootstrap PU & PEoU

Variable	***Mean***	***SD***	***CI_lower***	***CI_upper***
(Intercept)	2.926	0.859	0.926	4.183
PU	0.272	0.150	-0.036	0.552
PEoU	0.293	0.167	-0.016	0.647

4.2.3 Multivariate OLS models with controls

Table 9 examines the influence of PU, PEoU and awareness on investment in cybersecurity (NIST), including control variables. In model (1), which includes only PU, the coefficient is positive ($\beta = 0.288$), but not statistically significant. The standard error is 0.182, indicating limited precision of the estimation. While this suggests a positive influence of PU, it is not convincingly supported within this model.

Model (2) considers only PEoU, with a coefficient of $\beta = 0.317$ and a standard error of 0.211. The effect is positive but not significant. This indicates that PEoU by itself has limited explanatory power when controlling for other factors.

Model (3) combines PU and PEoU. Both coefficients remain positive (PU = 0.246; PEoU = 0.266) but again are not significant. The standard errors increase slightly (0.184 and 0.212), indicating possible multicollinearity, PU and PEoU are both conceptually and empirically related and may partly overlap in explanatory power. This overlap makes it difficult to accurately estimate the individual effects, which removes their statistical significance.

In model (4), an interaction term (PU_PEoU) is added, measuring the combined effect of PU and PEoU. This interaction term is significant ($\beta = 0.255$, $p < 0.05$) with a standard error of 0.124. This suggests that the combination of perceived usability and ease of use does matter for investment behaviour, possibly because the mutual reinforcement of these factors only becomes apparent when they are analysed together.

Model (5) uses a composite variable ‘Awareness’ calculated as the arithmetic mean of PU and PEoU. This is in line with the TAM, in which PU and PEoU jointly determine behavioural intention. The coefficient of this composite variable is significantly positive ($\beta = 0.509$, $p < 0.05$) with a standard error of 0.247. This suggests that higher levels of cybersecurity awareness are associated with greater willingness to invest.

The control variables (such as PMT, RBV, age, gender, IT responsibility, use of digital systems and province) are not significant in any of the models. Although their standard errors vary, their explanatory value is limited. Nevertheless, the explained variance (R^2) increases from 0.291 in

model (1) to 0.327 in models (4) and (5), with a corresponding increase in the adjusted R^2 to 0.153. This indicates improved model performance, despite the limited number of significance effects. The results in Table 9 show that especially the combination of PU and PEoU as a composite measure of awareness has a significant effect on investment readiness, while their separate effects do not. A possible explanation for this is that PU and PEoU are strongly interrelated, so their combined effect emerges more powerful and stable than when analysed separately.

Table 9: Awareness and Investment with Controls.

	Dependent variable:				
	Cybersecurity Investment (NIST)				
	PU	PEoU	PU+PEoU	Sum	Average
	(1)	(2)	(3)	(4)	(5)
PU	0.288		0.246		
	(0.182)		(0.184)		
PEoU		0.317	0.266		
		(0.211)	(0.212)		
PU_PEoU				0.255*	
				(0.124)	
Awareness					0.509*
					(0.247)
PMT	0.117	0.224	0.066	0.064	0.064
	(0.201)	(0.168)	(0.203)	(0.195)	(0.195)
RBV	-0.040	0.001	0.009	0.008	0.008
	(0.111)	(0.118)	(0.116)	(0.112)	(0.112)
Age	-0.092	-0.096	-0.106	-0.105	-0.105
	(0.211)	(0.212)	(0.210)	(0.206)	(0.206)
Gender	-0.149	0.027	-0.003	-0.009	-0.009
	(0.272)	(0.296)	(0.293)	(0.273)	(0.273)
IT-responsible	-0.068	-0.095	-0.100	-0.099	-0.099
	(0.094)	(0.098)	(0.097)	(0.094)	(0.094)
Systems	0.070	0.030	0.037	0.038	0.038
	(0.061)	(0.066)	(0.066)	(0.061)	(0.061)
Province	-0.012	-0.009	-0.012	-0.012	-0.012
	(0.017)	(0.017)	(0.017)	(0.016)	(0.016)
Constant	4.271***	3.576**	3.422*	3.448**	3.448**
	(1.097)	(1.291)	(1.280)	(1.196)	(1.196)
Observations	40	40	40	40	40
R^2	0.291	0.286	0.327	0.327	0.327
Adjusted R^2	0.108	0.102	0.125	0.153	0.153
Note:	*p**p***p<0.001				
	* p<0.001				

4.2.4 Interaction model: PU × PEoU on cybersecurity investment

Table 10 shows a regression model examining the interaction effect between PU and PEoU on cybersecurity investments, including control variables. The purpose of this model is to examine whether the combination of PU and PEoU has a strengthening or weakening effect on investment decisions.

Both PU and PEoU separately show negative but non-significant coefficients (PU: $\beta = -0.375$; PEoU: $\beta = -0.469$). The standard errors are relatively large (0.560 and 0.660, respectively), indicating a high degree of uncertainty in the estimates. This means that within this model, there is no convincing evidence for an independent effect of PU or PEoU on investment once the interaction effect is included. A possible explanation is that the inclusion of the interaction term leads to multicollinearity and increased variance in the estimates, making the individual effects of PU and PEoU more difficult to reliably isolate.

The interaction term PU*PEoU shows a positive effect ($\beta = 0.143$), but even this effect is not statistically significant (standard error = 0.122). Although the direction of the effect suggests that the combination of PU and PEoU is positively related to cybersecurity investments, the effect is too uncertain to draw firm conclusions. One possible explanation for the absence of significance is that the inclusion of the interaction term leads to higher variance and overestimation of standard errors, especially for a relatively small sample. Moreover, PU and PEoU are strongly related in content, which may lead to multicollinearity, making individual effects more difficult to isolate.

Non of the control variables are significant in this model. The coefficients are small and the standard errors relatively high, indicating limited explanatory value of these factors in this context. A possible explanation is that the influence of these control variables is small in this context or that the sample size is too small to reliably detect subtle effects.

Nevertheless, the model shows reasonable explanatory power. The R^2 value is 0.357, explaining about 36% of the variance in cybersecurity investments. The adjusted R^2 is 0.135, indicating a slight correction for the number of included variables, but still indicating a functional model.

Finally, the constant in the model is significant ($\beta = 6.169$, $p < 0.05$), with a relatively large standard error (2.663). This suggests that the baseline level of investment is substantial even when all explanatory variables are set to zero.

*Table 10: Interaction-effect PU*PEoU on NIST (with control)*

	Dependent variable:
	Cybersecurity Investment (NIST)
	Interaction model
PU	-0.375
	(0.560)
PEoU	-0.469
	(0.660)
PMT	0.069
	(0.202)
RBV	0.025
	(0.116)
Age	-0.078
	(0.210)
Gender	-0.035
	(0.293)
IT-responsible	-0.063
	(0.101)
Systems	0.052
	(0.067)
Province	-0.013
	(0.017)
PU:PEoU	0.143
	(0.122)
Constant	6.169*
	(2.663)
Observations	40
R^2	0.357
Adjusted R^2	0.135
Note:	*p**p***p<0.001
	* p<0.001

5 Conclusion and limitations

5.1 Summary of findings

The first finding is that both PU and PEoU separately show a positive and significant effect on investment level in a single OLS model without control variables. PU has a significant positive effect in this model ($\beta = 0.377$, $p < 0.001$), as well as PEoU ($\beta = 0.411$, $p < 0.001$). These results suggest that respondents who perceive cybersecurity measures as useful and user-friendly are more likely to invest in such measures.

The second finding concerns the combined model that includes both PU and PEoU simultaneously. Although both coefficients remain positive, their separate significances disappear. This is explained by multicollinearity: PU and PEoU are conceptually and empirically correlated ($r = 0.55$), leading to overlapping explanatory power. Nevertheless, the model with both variables together shows a higher explained variance ($R^2 = 0.274$), indicating a robust combined effect. These findings imply that the combined effect of perceived utility and ease of use provides more insight into investment propensity than either factor separately, as their combined inclusion in the model leads to a higher explained variance despite the loss of separate significance.

The third finding follows from the bootstrap analysis, which further tested the reliability of the relationship between PU, PEoU and investment behaviour. Although the mean coefficients of both variables remain positive (PU = 0.272, PEoU = 0.293), the confidence intervals include the number zero. As a result, the effects are not statistically significant, which can largely be attributed to the small sample size ($n = 40$) and the shared explanatory variance between the core variables.

The fourth finding concerns the multivariate regression model with control variables. Neither PU nor PEoU separately is found to have a significant effect. However, when PU and PEoU are combined in a composite variable for cybersecurity awareness (mean score), it does appear to be significantly and positively associated with investment level ($\beta = 0.509$, $p < 0.05$), with increased explained variance ($R^2 = 0.327$). It is not individual impressions but overall awareness that determines whether companies want to invest.

The fifth and final finding comes from the interaction model, which examines the interaction between PU and PEoU. Although the interaction term suggests a positive effect ($\beta = 0.143$), it is not statistically significant. This suggests that the reinforcing effect of ease of use on the usefulness

of cybersecurity measures has not been convincingly demonstrated in this sample. This may be due to the limited sample size and associated standard errors.

5.2 Theoretical implications

The findings of this study provide important theoretical implications. The first contribution of this research concerns the available literature on cybersecurity awareness. Existing studies identify a gap between awareness of cyber threats and actual protection measures within SMEs, but little quantitative research exists to date on the impact of this awareness on investment behaviour (Chidukwani, Zander, & Koutsakis, 2022). Chidukwani, Zander & Koutsakis (2022) note that quantitative research on cybersecurity in SMEs is still underrepresented and argue for the use of quantitative methods, especially focusing on features such as practical implementation of security measures which in this study was measured by the variable PEoU. By examining this relationship in practice among SMEs, this thesis helps to fill a gap in the existing literature. The results show that cybersecurity awareness, measured through the constructs PU and PEoU, is positively related to the level of investment in cybersecurity measures, confirming that awareness plays a role in strategic decision-making.

Secondly, this study contributes to the lack of research done so far in the field of cybersecurity investment in the Netherlands. While most existing studies focus on large enterprises or international contexts, this study explicitly focuses on SME retailers in the Netherlands, a sector that, while digitally vulnerable, is often outside the scope of regulations such as the NIS2 directive. As such, this study offers new insights into how unregulated companies deal with cyber threats and what role awareness plays in this. This reinforces the case for more context-specific research within SMEs, as previously suggested by Furnell & Clarke (2012). The theoretical relevance of this research is reinforced by findings from another study conducted by ABN AMRO (2025), which shows that one in five Dutch companies fell victim to a cyber-attack in 2024 and that SMEs are often insufficiently familiar with the NIS2 directive (Krauwer, 2025). Whereas the ABN AMRO survey gives general information of cybersecurity issues among Dutch businesses, this thesis offers more depth insights into the underlying behavioural factors that influence investment decisions within SME retailers. By measuring cybersecurity awareness through PU and PEoU, this research makes a theoretical contribution by showing how individual perceptions of utility and ease of use are related to investment readiness in an industry outside of formal regulation.

In summary, this research adds theoretical value by empirically demonstrating the effect of cybersecurity awareness on investment behaviour and adding to the literature on SME cybersecurity in an under-researched and policy-relevant sector.

5.3 Managerial and practical implications

The results of this study contain several relevant managerial and practical implications.

First, the findings suggest that policymakers can shape their cybersecurity awareness efforts within SMEs more specifically and effectively. This research shows that higher cybersecurity awareness scores are significantly associated with higher willingness to invest in cybersecurity measures. This implies that government programs and information campaigns are more effective when they focus not only on general warnings about cyber threats, but especially on clarifying how security measures are useful and can be practically applied by SMEs.

Second, the results offer starting points for policy interventions in sectors outside the scope of the NIS2 directive, such as the Dutch retail sector. As these companies are not legally obliged to implement cybersecurity measures, their willingness to invest mainly depends on voluntary motivation and internal conviction. This study shows that awareness, even in the absence of legislation, does have a positive effect on investment behaviour. This implies that awareness campaigns can stimulate behavioural change, provided they focus on understandable, accessible and context-relevant information about digital resilience. This policy assumption is confirmed in the Dutch Cybersecurity Strategy (2022-2028), but so far received little empirical support. This study shows that awareness within SMEs is related to willingness to invest.

Third, the findings of this study offer concrete tools for retail entrepreneurs, industry associations and policymakers alike. Focusing internal training and communication on increasing the perceived usefulness and ease of use of cybersecurity measures can raise employee awareness and increase investment readiness. At the same time, policymakers can use public resources more effectively by focusing on these modifiable factors, thereby strengthening digital resilience within SMEs in a more targeted and efficient manner.

5.4 Limitations and future research

This study has several limitations that provide valuable insights and directions for future research.

A first limitation concerns the size and representativeness of the sample. The analysis is based on only 40 respondents who met the selection criteria. Such a small sample size entails important limitations for both statistical power and generalisability of the results. Small sample sizes reduce the likelihood of detecting significant effects, potentially allowing true relationships to go undetected (Etz & Arroyo, 2015). Studies with too small sample sizes also risk generating misleading or unreliable conclusions due to insufficient statistical precision (SPRINT Investigators, 2012). Cook's Distance analysis was performed to see if any observations were overly influential on the regression; this is the case. Due to the limited sample size, all these observations were retained, including the data points identified as potentially influential according to Cook's Distance. *Appendix 7.2* presents the results of the Cook's Distance analysis, showing that eight observations exhibit a value above the threshold of 1/n. These influential data points are visually identifiable as the bars protruding above the red reference line. Researchers conducting future studies with larger datasets may decide to exclude such influential cases or analyse them separately to increase the robustness of the results and internal validity. In this study, several effects, although theoretically relevant and substantively consistent with expectations, were found to be statistically insignificant. This makes it difficult to draw robust conclusions. To quantify the statistical limitations of the sample size, a post-hoc power analysis was performed (see *appendix 7.3*). The analysis shows that the model has only 28% power to detect a mean effect (Cohen's $f^2 = 0.15$), which is well below the usual lower limit of 80%. This highlights the need to interpret non-significant results with caution. These limitations also provide valuable directions for future research, in which larger and more representative samples can be used to test the theoretically expected relationships.

In addition to this point, the sampling method is a potential source of selection bias, which is an additional threat to external validity. When participants self-report, there is a possibility that certain types of respondents are unknowingly over-represented, for example entrepreneurs with a greater interest in or awareness of cybersecurity. This leads to a systematic deviation from the target population (Chen, Keglovits, Devine, & Stark, 2022). Convenience samples may in this way lead to conclusions that should not be generalised to the broader population without question (Boyd,

Powney, & Pescott, 2023). Future research may overcome this limitation by using random sampling to better determine the extent to which the relationships found are representative of the broader population of SME retailers within the Netherlands.

A second limitation concerns the lack of bootstrapping capabilities for all (control) variables. Due to the small sample size and categorical control variables, it was not possible to test the full regression models with bootstrap analyses. The robustness of some findings, especially in models with many control variables, could therefore not be fully established. Future research with larger samples may resolve this while enabling broader robustness testing.

A third limitation concerns the wording of some survey items. Several statements contain compound wording or interpretation-sensitive language, such as the use of words like ‘and’ or ‘sometimes’, which can lead to interpretation differences and noise in the measurement results. Such formulations complicate unambiguous interpretation of responses and may affect the internal consistency of the scales. Future research can be improved by better testing the questionnaire and making the questions clearer to reduce measurement errors.

Furthermore, this study focuses exclusively on individual perceptions of PU and PEoU based on the TAM, it excludes other relevant theoretical perspectives such as PMT and RBV in the main variable. As a result, psychological motivations such as threat perception and self-efficacy (Rogers, 1975; Floyd, Prentice-Dunn, & Rogers, 2000), as well as strategic organisational characteristics such as internal capabilities and resources (Weishäupl, Yasasin, & Schryen, 2015; Madhani, 2010), remain underexposed. For follow-up research, it may be valuable to still include these theoretical frameworks, as they may offer additional explanations for cybersecurity investment behaviour within SMEs. Combining the different models was not done in this study because it could cause theoretical inconsistency, but the insights from these omitted models could be valuable for the outcome of the research question.

Finally, the cross-sectional design of this study constitutes a methodological limitation. Because all data were collected at a single point in time, changes in awareness or willingness to invest over time cannot be determined. Nor is it possible to make statements about causality. Longitudinal research could help not only to chart the course of cybersecurity awareness and investment behaviour, but also to evaluate the effectiveness of policy interventions and awareness campaigns over time. Future research thus offers an opportunity to understand how the relationship between awareness and investment behaviour develops over time.

These limitations offer valuable starting points for future research. For instance, using larger and randomly drawn samples may help to test the theoretically expected relationships more robustly and increase representativeness against the broader population of Dutch SME retailers. In addition, it is recommended to further test and refine the questionnaire to minimise measurement errors. Finally, longitudinal follow-up research can provide insight into how the relationship between awareness and investment behaviour develops over time.

5.5 Conclusion

This study investigated the influence of cybersecurity awareness on Dutch SME retailers' willingness to invest in cybersecurity measures. Within this context, the relationship between awareness and investment behaviour was empirically analysed using a survey with 40 valid respondents, using the Technology Acceptance Model.

The results show that cybersecurity awareness, operationalized through the perceptions of PU and PeoU, is positively related to level of investment in cybersecurity measures. In single regression models, both PU and PEoU are found to be individually significant. In multivariate models, this significance disappears, but when PU and PEoU are combined into a composite awareness variable, this combination does turn out to be a significant predictor of investment behaviour. This suggests that SME retailers are more likely to invest when they see cybersecurity as both useful and easy to implement. Despite methodological limitations, this research provides valuable insights for both theory and practice. The findings underline the importance of awareness-raising interventions that not only communicate threats but also clarify how and why cybersecurity measures are effective and feasible for small businesses. The central research question of this study was:

Does the level of cybersecurity awareness affect investment in cybersecurity measures within small and medium-sized enterprises in the retail sector in the Netherlands?

Based on the findings, it can be concluded that a higher level of cybersecurity awareness leads to a higher amount of investment. Awareness is a critical prerequisite for taking protective measures, even in a context without direct legal obligation. H1 can be assumed based on this study, but with some caution due to the small sample size, the lack of significant effects in loose variables and the limited robustness test.

This conclusion underlines the importance of accessible and practical awareness campaigns targeting SMEs as a strategic tool in strengthening digital resilience. From awareness to action, awareness is not an end, but a necessary condition for achieving digital resilience, even in sectors without legal obligations such as the SME Retail sector in the Netherlands.

6 References

Al-Janabi, S. (2016). *A Study of Cyber Security Awareness in Educational Environment in the Middle East.* World Scientific. Retrieved from http://dx.doi.org/10.1142/S0219649216500076

Almuhammadi, S., & Alsaleh, M. (2017). *Information security maturity model for NIST cyber security framework.* doi:10.5121/csit.2017.70305

Anwar, M., He, W., Ash, I., Yuan, X., & Li, L. (2017). *Gender Difference and Employees' Cybersecurity Behaviors.* doi:https://doi.org/10.1016/j.chb.2016.12.040

Boyd, R., Powney, G., & Pescott, O. (2023). *We need to talk about nonprobability samples.* Retrieved from https://doi.org/10.1016/j.tree.2023.01.001

Centraal Bureau voor de Statistiek. (2024, 06 28). *Cybersecuritymonitor 2023*. Retrieved from https://www.cbs.nl/nl-nl/longread/rapportages/2024/cybersecuritymonitor-2023?onepage=true

Chen, S.-W., Keglovits, M., Devine, M., & Stark, S. (2022). *Sociodemographic Differences in Respondent Preferences for Survey Formats: Sampling Bias and Potential Threats to External Validity.* Retrieved from https://doi.org/10.1016/j.arrct.2021.100175

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). *A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations.* IEEEAccess. Retrieved from https://doi.org/10.1109/ACCESS.2022.3197899

Cobos, E. V. (2024). *Cybersecurity Economics for Emerging Markets.* World Bank Group. doi::10.1596/978-1-4648-2120-2

Cook, D. (2011). *Encyclopedia of Statistical Science.* Springer. doi:10.1007/978-3-642-04898-2

Cyber Security Raad. (2024, 06 04). *Cyber Security Raad: de cyberweerbaarheid van het mkb moet versterkt*. Retrieved from Cyber Security Raad: https://www.cybersecurityraad.nl/documenten/adviezen/2024/06/04/csr-advies-verkleinen-van-de-cyberweerbaarheidskloof

Davis, F. (1987). *Technology acceptance model: TAM.* Retrieved from https://quod.lib.umich.edu/b/busadwp/images/b/1/4/b1409190.0001.001.pdf

Digital Government. (2025, 01 17). *Wees voorbereid*. Retrieved from Digitale Overheid: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/wees-voorbereid/

Digitale Overheid. (2019, 10 29). *"Onszelf wapenen tegen gevolgen van digitale ontwrichting"*. Retrieved from Digitale Overheid : https://www.digitaleoverheid.nl/achtergrondartikelen/overheidsbrede-cyberoefening-oefenen-om-ons-te-wapenen-tegen-gevolgen-van-digitale-ontwrichting/

Digitale Overheid. (n.d.). *NIS2-richtlijn*. Retrieved from Digitale Overheid: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn/

Duanmu, X., Yuan, X., Zhang, X., & Yu, J. (2025). *How Does Digital Infrastructure Mitigate Urban-Rural Disparities.* Retrieved from https://doi.org/10.3390/su17041561

Etz, K., & Arroyo, J. (2015). *Small Sample Research: Considerations Beyond Statistical Power.* Retrieved from https://doi.org/10.1007/s11121-015-0585-4

European Commission. (2022). *NIS2 Directive: new rules on cybersecurity of network and information systems*. (European Union) Retrieved from European Commission: The NIS2 Directive requires medium and large enterprises within critical sectors to implement enhanced cybersecurity measures, incident reporting and adherence to national strategies to promote cyber resilience. Member states are charged with monitoring c

European Commission. (2022). *NIS2 Directive: new rules on cybersecurity of network and information systems*. Retrieved from European Commission: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Fallatah, W., Kävrestad, J., & Furnell, S. (2024). *Establishing a Model for the User Acceptance of Cybersecurity Training.* Retrieved from https://doi.org/10.3390/fi16080294

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). *A Meta-Analysis of Research on Protection Motivation Theory.* Retrieved from https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Furnell, S., & Clarke, N. (2012). *Power to the people? The evolving recogition of human aspects of security.* SciVerse ScienceDirect. Retrieved from https://doi.org/10.1016/j.cose.2012.08.004

Government of the Netherlands. (2024, 10 16). *NIS2 Zelfevalutatie NL*. Retrieved from Regelhulpenvoorbedrijven: https://regelhulpenvoorbedrijven.nl/NIS-2-NL/

Haeussinger, F., & Kranz, J. (2013). *Information security awareness: Its antecedents and mediating effects on security compliant behavior.* Retrieved from https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=562b160c858a35ffcd02e0726835cf1000bca91e

Heidt, M., Gerlach, J., & Buxmann, P. (2019). *Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments.* Retrieved from https://doi.org/10.1007/s10796-019-09959-1

Hesterberg, T. (2011). *Bootstrap.* Retrieved from https://doi.org/10.1002/wics.182

Holden, R. J., & Karsh, B.-T. (2010). *The Technology Acceptance Model: Its past and its future in health care.* Retrieved from https://doi.org/10.1016/j.jbi.2009.07.002

Jamil, H., Zia, T., Nayeem, T., Whitty, M., & Alessandro, S. (2025). *Human-centric cyber security: Applying protection motivation theory to analyse micro business owners' security behaviours.* Emerald Insight. Retrieved from https://doi.org/10.1108/ICS-10-2023-0176

Khan, N., Ikram, N., & Saleem, S. (2023). *Effects of socioeconomic and digital inequalities on cybersecurity in a developing country.* PMC PubMed Central. doi:10.1057/s41284-023-00375-4

Koopal, H. (2025, 05 21). *Eén op de vijf Nederlandse bedrijven leed in 2024 schade door cyberaanval*. Retrieved from ABN AMRO: https://www.abnamro.com/nl/nieuws/een-op-de-vijf-nederlandse-bedrijven-leed-in-2024-schade-door-cyberaanval

Kopp, E., Wilson, C., & Kaffenberger, L. (2017). *Cyber risk, market failures, and financial stability.* International Monetary Fund. Retrieved from https://books.google.it/books?hl=nl&lr=&id=0L1ADwAAQBAJ&oi=fnd&pg=PA3&dq=%09+Cyber+Risk,+Market+Failures,+and+Financial+Stability&ots=qdEhaqigq3&sig=6BZe85U1nh_VnyUAseEdvnZgPJE&redir_esc=y#v=onepage&q=Cyber%20Risk%2C%20Market%20Failures%2C%20and%20Financi

Krauwer, J. (2025, 05 21). *Eén op de vijf Nederlandse bedrijven leed in 2024 schade door cyberaanval*. (H. Sjouke Koopal, Editor, & ABN AMRO) Retrieved from ABN AMRO:

https://www.abnamro.com/nl/nieuws/een-op-de-vijf-nederlandse-bedrijven-leed-in-2024-schade-door-cyberaanval

Levy, M., & Grewal, D. (2023). *Retailing Management* (eleventh edition ed.). MC Graw Hill. Retrieved from https://thuvienso.hoasen.edu.vn/bitstream/handle/123456789/13140/Contents.pdf?sequence=1

Liu, X., Ahmad, S., Anser, M., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). *Cyber security threats: A never-ending challenge for e-commerce.* doi:10.3389/fpsyg.2022.927398

Madhani, P. M. (2010). *Resource Based View (RBV) of Competitive Advantage: An Overview.* SSRN. Retrieved from https://ssrn.com/abstract=1578704

Ministry of Justice and Security. (2024, 12 03). Staatsblad van het Koninkrijk der Nederlanden. *Jaargang 2024, nummer 52*, p. 8. Retrieved from https://zoek.officielebekendmakingen.nl/stb-2024-52.html#:~:text=Het%20besluit%20verhoogt%20de%20twee,van%20inflatie%20en%20bedraagt%2025%25.

Moore, T., Dynes, S., & Chang, F. R. (2015). *Identifying How Firms Manage Cybersecurity Investment.* Retrieved from https://tylermoore.ens.utulsa.edu/ciso15ibm.pdf

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2021). *Cybersecuritybeeld Nederland.* Ministerie van Justitie en Veiligheid. Retrieved from https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2022). *Cybersecuritybeeld Nederland.* Ministerie van Justitie en Veiligheid. Retrieved from https://www.nctv.nl/documenten/publicaties/2022/07/04/cybersecuritybeeld-nederland-2022

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2023). *Cybersecuritybeeld Nederland 2023.* Ministerie van Justitie en Veiligheid. Retrieved from https://www.nctv.nl/documenten/publicaties/2023/07/03/cybersecuritybeeld-nederland-2023

National Cyber Security Centre. (2022, 10 10). Retrieved from Ministerie van Justitie en Veiligheid: https://www.ncsc.nl/over-ncsc/documenten/publicaties/2022/oktober/10/actieplan-nederlandse-cybersecuritystrategie-2022-2028

National Cyber Security Centre. (2023). *Omgaan met risico's in de toeleveringsketen.* Ministerie van Justitie en Veiligheid. Retrieved from https://www.ncsc.nl/documenten/publicaties/2023/augustus/15/risicos-in-de-toeleveringsketen

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity.* Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Retail Federation. (2023). *Retail Security Survey.* National Retail Federation & Loss Prevention Research Council. Retrieved from https://nrf.com/research/national-retail-security-survey-2023

Nurqamarani, A. S., Soegiarto, E., & Nurlaeli. (2021). *Technology Adoption in Small-Medium Enterprises based on Technology Acceptance Model: A Critical Review.* Journal of Information Systems Engineering and Business Intelligence. Retrieved from http://dx.doi.org/10.20473/jisebi.7.2.162-172

Renaud, K., & Ophoff, J. (2021). *A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs.* Retrieved from https://doi.org/10.1108/OCJ-03-2021-0004

Rogers, R. W. (1975). *A Protection Motivation Theory of Fear Appeals and Attitude Change1.* doi:10.1080/00223980.1975.9915803

Rombaldo, C., Becker, I., & Johnson, S. (2023). *Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity.* London. doi:10.48550/arXiv.2309.17186

Ruohonemr, J. (2024). *A Systematic Literature Review on the NIS2 Directive.* University of Southern Denmark, Sønderborg. Sønderborg: Arxiv - Cornell University. Retrieved from https://doi.org/10.48550/arXiv.2412.08084

Saeed, S., Altamimi, S., Alkayyal, n., Alshehri, E., & Alabbad, D. (2023). *Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations.* Retrieved from https://doi.org/10.3390/s23156666

Scofield, M. (2016). *Benefiting form the NIST Cybersecurity Framework.* Retrieved from https://www.proquest.com/openview/e54ef43df41838caa8c37926ed106690/1?cbl=47365&pq-origsite=gscholar

Shojaifar, A., & Järvinen, H. (2021). *Classifying SMEs for Approaching Cybersecurity Competence and Awareness.* ACM Digital Library. Retrieved from https://doi.org/10.1145/3465481.3469200

Sohn, K., & Kwon, O. (2019). *Technology acceptance theories and factors influencing artificial.* Telematics and Informatics. Retrieved from https://doi.org/10.1016/j.tele.2019.101324

SPRINT Investigators. (2012). *(Sample) Size Matters! An Examination of Sample Size From the SPRINT Trial Study to Prospectively Evaluate Reamed Intramedullary Nails in Patients With Tibial Fractures.* doi:10.1097/BOT.0b013e3182647e0e

Straub, D. (1990). *Effective IS Security: An Empirical Study.* ResearchGate. Retrieved from http://dx.doi.org/10.1287/isre.1.3.255

Symantec. (n.d.). *Cyber Security for Retail Services.* Symantec. Retrieved from https://docs.broadcom.com/doc/cybersecurity-retail-en

Tavakol, M., & Dennick, R. (2011). *Making sense of Cronbach's alpha.* Retrieved from https://doi.org/10.5116/ijme.4dfb.8dfd

Thales. (2022). *2022 Thales Data Threat Report*. Retrieved from https://cpl.thalesgroup.com/sites/default/files/content/research_reports_white_papers/field_document/2022-11/2022-data-threat-report-retail-edition.pdf

The Netherlands Enterprise Agency. (2025). *Meer bedrijven in kritieke sectoren krijgen verplichtingen voor cyberbeveiliging (NIS2)*. Retrieved from Ondermnemersplein: https://ondernemersplein.kvk.nl/nis2-richtlijn-beschermt-netwerk-en-informatiesystemen-tegen-cyberbeveiligingsrisicos/

Vaka, P. (2025). *International Research Journal of Modernization in Engineering Technology and Science.* Irjmets. Retrieved from https://www.doi.org/10.56726/IRJMETS67237

van der Kleij, R. (2018). *Hoe cyberweerbaar zijn mkb-retailers?* De Haagse Hogeschool. Retrieved from https://www.dehaagsehogeschool.nl/media/cyberweerbaarheid-mkb#:~:text=Slachtofferschap%20van%20cybercrime%20Bijna%20de,gevolg%20van%20cybercriminaliteit%20kan%20zich

Van der Kleij, R., De Bruin, I., Van 't Hoff-de Goede, S., Ancher, M., & Leukfeldt, R. (2019, 03 04). *Cybercriminaliteit leeft niet onder retailers*. Retrieved from Centrum voor criminaliteitspreventie en veiligheid: https://ccv-secondant.nl/platform/article/cybercriminaliteit-leeft-niet-onder-retailers#:~:text=Het%20midden,heeft%20bovendien%20schade%20hiervan%20onderv onden

Verbrugge, R. (2025, 05 21). *Eén op de vijf Nederlandse bedrijven leed in 2024 schade door cyberaanval*. Retrieved from ABN AMRO: https://www.abnamro.com/nl/nieuws/een-op-de-vijf-nederlandse-bedrijven-leed-in-2024-schade-door-cyberaanval

Vrhovec, S., & Markelj, B. (2024). *We need to aim at the top: Factors associated with cybersecurity awareness of cyber and information security decision-makers.* Retrieved from https://doi.org/10.1371/journal.pone.0312266

Weishäupl, E., Yasasin, E., & Schryen, G. (2015). *IT Security Investments through the Lens of the Resource-based View: A new theoretical Model and Literature Review.* Retrieved from https://epub.uni-regensburg.de/31402/1/IT%20SECURITY%20INVESTMENTS%20THROUGH%20THE%20LENS%20OF%20THE%20RESOURCE-BASED%20VIEW%20A%20NEW%20THEORETICAL%20MODEL%20AND%20LITERATURE%20REVIEW%20-%20final%20version.pdf

White, H. (1980). *A heteroskedasticity-consistent covariance matrix estimator and a direct test for heteroskedasticity.* Retrieved from https://doi.org/10.2307/1912934

World Economic Forum. (2016). *Understanding Systemic Cyber Risk.* Retrieved from https://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf

Zwilling, M., Wiechetek, L., Lesjak, D., & Çetin, F. (2022). *Cyber Security Awareness, Knowledge and Behavior: A Comparative Study.* ResearchGata. Retrieved from http://dx.doi.org/10.1080/08874417.2020.1712269

7 Appendix

7.1 Survey

The survey was administered in Dutch, as the target group consisted of Dutch SME retailers. This choice was made to minimise the risk of language-related miscommunication and to maximise response rates. Since the phrasing of several survey items is discussed in the section Limitations and Future Research, the full survey is included twice in this appendix: first in English, the language of this thesis, followed by the original Dutch version in which the data were actually collected. This dual inclusion serves to enhance the transparency and replicability of the research.

7.1.1: Translated survey (English)

Introduction

Dear participant,

You are invited to take part in a survey conducted as part of a master's thesis project in Financial Economics at Radboud University. This research focuses on the extent to which cybersecurity awareness influences investments in security measures within the Netherlands.

The study is socially relevant, as it contributes to a better understanding of the factors that drive businesses to protect themselves against digital threats. In a time when cyberattacks are becoming increasingly frequent and sophisticated, it is important to understand what motivates entrepreneurs to take action. Your input will help to map this out more clearly.

Completing the questionnaire will take approximately 10 minutes.

Your participation is completely anonymous. The data will be used solely for academic purposes and cannot be traced back to individual persons or companies.

Among all participants, two €25 bol.com gift cards will be raffled as a token of appreciation for your participation.

At the end of the survey, you may – if you wish – enter your email address to participate in this raffle. This email address will be processed separately from your survey responses.

Your cooperation is of great value to the success of this research. Thank you very much for your time and contribution!

The survey starts on the next page. If you have any questions or comments, please contact the researcher, Max Masselink, at max.masselink@ru.nl. Once again, thank you very much for your participation.

The retail sector is engaged in the sale of goods and services to consumers, both through physical stores and online channels.

Does your company operate within the retail sector?

- Yes
- No

Where is your company located?

- (If your company is located in multiple provinces, you may select more than one answer.) Drenthe
- Flevoland
- Friesland
- Gelderland
- Groningen
- Limburg
- Noord-Brabant
- Noord-Holland
- Overijssel
- Utrecht
- Zeeland
- Zuid-Holland
- Not in The Netherlands

Categorie	Netto-omzet (€)	Balanstotaal (€)	Aantal werknemers (FTE)
A.	0 – 900.000	0 – 450.000	0 – 10
B.	900.001 – 15.000.000	450.001 – 7.500.000	11 – 50
C.	15.000.001 – 50.000.000	7.500.001 – 25.000.000	51 – 250
D.	> 50.000.000	> 25.000.000	> 250

To determine the correct category of your company, this study uses the size of your business. That size is determined based on three criteria:

1. **Net turnover:** This is the money your company earned from sales, excluding VAT and discounts.
2. **Balance sheet total:** This is the total value of everything your company owns and owes.
3. **Number of employees (FTE):** This is the number of people working full-time at your company, including part-timers converted to full-time equivalents.
   There are four categories (A, B, C and D). Your company falls into a certain category if it meets at least two of the three criteria listed above.

Which category did your company fall into in the previous financial year?
Note: Your company falls into a specific category if it meets at least two of the three criteria. (You may provide an estimate if you do not know the exact figures.)

- Category A
- Category B
- Category C
- Category D
- Your company does not meet at least two of the three criteria for any of the four categories

Which category did your company fall into two financial years ago?
Note: Your company falls into a specific category if it meets at least two of the three criteria. (You may provide an estimate if you do not know the exact figures.)

- Category A
- Category B
- Category C
- Category D
- Your company does not meet at least two of the three criteria for any of the four categories

Control variables:

What is your role within the organisation?

- Owner / Director
- IT Manager / ICT Responsible
- Financial Responsible
- Administrative Staff
- Sales / Shop Floor Staff
- Other, namely: _____

What is your age?

- Under 25 years
- 25–34 years
- 35–44 years
- 45–54 years
- 55–64 years
- 65 years or older

What is your gender?

- Male
- Female
- Prefer not to say
- Other, namely: _____

Does your organisation use digital systems for core activities (such as inventory management, customer communication or payments)?

- Yes, for multiple core activities
- Yes, for some core activities
- No
- I don’t know

Does your organisation have an employee or external party responsible for IT or cybersecurity?

- Yes, an internal employee
- Yes, an external service provider
- Yes, both internal and external
- No, no one is specifically responsible for this
- I don’t know

Through which channel(s) is your company primarily active in customer contact and/or sales of products or services?

- Physical only (e.g. through stores, fairs or office locations)

- Online only (e.g. through a webshop, app or platform)
- Both physical and online
- Other, namely: _____

For all statements below:

(1) Strongly disagree
(2) Disagree
(3) Somewhat disagree
(4) Neutral
(5) Somewhat agree
(6) Agree
(7) Strongly agree
(8) Do not know / No opinion

Geef aan in hoeverre de onderstaande uitspraken van toepassing zijn op u of op uw organisatie.

RBV:

Our investments in cybersecurity visibly lead to better performance or reduced risks within our company.

(1) (2) (3) (4) (5) (6) (7) (8)

The way our people, processes and technology come together in the area of cybersecurity is unique.

(1) (2) (3) (4) (5) (6) (7) (8)

In our company, cybersecurity is seen as an important strategic tool, not just as an IT cost or obligation.

(1) (2) (3) (4) (5) (6) (7) (8)

PMT:

A cyberattack on our company could have major consequences.

(1) (2) (3) (4) (5) (6) (7) (8)

I believe that cybersecurity measures can effectively protect our company against digital threats.

(1) (2) (3) (4) (5) (6) (7) (8)

I intend to actively protect our company against cyber threats.

(1) (2) (3) (4) (5) (6) (7) (8)

PU:

Cybersecurity measures help me maintain control over important processes in my company.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecurity measures allow me to act faster and more effectively when something goes wrong, such as during a digital attack.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecurity helps keep my business running, even in difficult situations.

(1) (2) (3) (4) (5) (6) (7) (8)

Thanks to good cybersecurity, I work with a greater sense of security and peace of mind.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecurity tools are useful for effectively managing risks within my business.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecurity helps me make better decisions because I have more and better information.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecurity tools ensure that my digital processes run more smoothly and efficiently.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecurity improves the quality of how I manage my business.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecurity measures give me more control over my daily operations.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecurity measures allow me to complete my tasks more quickly.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecurity supports important aspects of my work.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecurity measures make my work more effective.

(1) (2) (3) (4) (5) (6) (7) (8)

Thanks to good cybersecurity, I can perform better in my job.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecurity makes it easier to do my job well.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecurity measures are useful for the daily running of my business.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecurity measures make me more productive.

(1) (2) (3) (4) (5) (6) (7) (8)

PEoU:

It is easy for me or my company to implement cybersecurity measures.

(1) (2) (3) (4) (5) (6) (7) (8)

I feel comfortable using cybersecurity tools or guidelines.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecurity measures are flexible and adapt well to our needs.

(1) (2) (3) (4) (5) (6) (7) (8)

I can easily do what I want with the available security measures.

(1) (2) (3) (4) (5) (6) (7) (8)

Performing security tasks is easy with the cybersecurity measures we use.

(1) (2) (3) (4) (5) (6) (7) (8)

I often find cybersecurity measures difficult to use.

(1) (2) (3) (4) (5) (6) (7) (8)

Working with cybersecurity measures is sometimes frustrating.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecurity measures are often not flexible and hard to adapt to our way of working.

(1) (2) (3) (4) (5) (6) (7) (8)

It takes a lot of effort and focus to properly use cybersecurity measures.

(1) (2) (3) (4) (5) (6) (7) (8)

It takes a lot of time and effort to learn to use cybersecurity measures properly.

(1) (2) (3) (4) (5) (6) (7) (8)

I don't need to think much about how to use cybersecurity measures.

(1) (2) (3) (4) (5) (6) (7) (8)

The rules and steps around cybersecurity are clear and easy to understand.

(1) (2) (3) (4) (5) (6) (7) (8)

It is easy to apply cybersecurity measures correctly in my business.

(1) (2) (3) (4) (5) (6) (7) (8)

Navigating cybersecurity tools is easy.

(1) (2) (3) (4) (5) (6) (7) (8)

I easily remember how to carry out security tasks.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecurity measures are generally easy to use.

(1) (2) (3) (4) (5) (6) (7) (8)

NIST:

We have a clear and up-to-date overview of all IT systems, software, and devices used within our company. (1) (2) (3) (4) (5) (6) (7) (8)

We know exactly which digital data and systems are most important to keep our operations running.

(1) (2) (3) (4) (5) (6) (7) (8)

In the past year, a serious and structured assessment of cybersecurity risks was conducted, and the results were documented. (1) (2) (3) (4) (5) (6) (7) (8)

Our employees regularly receive training or explanations about safe online behavior and cybersecurity.

(1) (2) (3) (4) (5) (6) (7) (8)

All devices and accounts in our company are well protected with strong passwords and/or two-factor authentication (e.g. an extra code via SMS or email).

(1) (2) (3) (4) (5) (6) (7) (8)

We regularly back up important data and check whether those backups actually work.

(1) (2) (3) (4) (5) (6) (7) (8)

We use antivirus software and firewalls, and they are regularly updated.

(1) (2) (3) (4) (5) (6) (7) (8)

We use software or tools to detect unusual or suspicious activity on our computer network.

(1) (2) (3) (4) (5) (6) (7) (8)

Within our company, it is clear what to do when someone notices something suspicious, such as a phishing email or hacking attempt.

(1) (2) (3) (4) (5) (6) (7) (8)

Our company has a clear step-by-step plan in place in case we face a cyberattack or other digital incident.

(1) (2) (3) (4) (5) (6) (7) (8)

Our employees know what to do when a cyber incident occurs (such as a hack or data breach).

(1) (2) (3) (4) (5) (6) (7) (8)

If we have experienced a cyber incident in the past, we evaluate afterwards what went well and what didn't to improve our response next time.

(1) (2) (3) (4) (5) (6) (7) (8)

We have a recovery plan in place for restoring systems after an attack.

(1) (2) (3) (4) (5) (6) (7) (8)

Our company has invested in measures that allow us to quickly recover from a cyberattack.

(1) (2) (3) (4) (5) (6) (7) (8)

Voucher raffle

Would you like to enter the raffle for a Bol.com gift card after completing this survey?

The winner will be contacted by email. Please leave your email address below.

If you provide your email here, it will be used solely for the purpose of the raffle.

- No
- Yes, my email address is: _____

Closure

We thank you for your time spent taking this survey.

Your response has been recorded.

7.1.2: Original survey (Dutch)

Introduction

Beste deelnemer,

U wordt uitgenodigd om deel te nemen aan een enquête in het kader van een afstudeeronderzoek voor de masteropleiding Financial Economics aan de Radboud Universiteit. Dit onderzoek richt zich op de vraag in welke mate het bewustzijn van cybersecurity van invloed is op de investeringen in beveiligingsmaatregelen binnen in Nederland.

Het onderzoek is maatschappelijk relevant, omdat het bijdraagt aan het inzicht in de factoren die er toe leiden dat bedrijven zich wapenen tegen digitale dreigingen. In een tijd waarin cyberaanvallen steeds frequenter en geraffineerder worden, is het belangrijk te begrijpen welke factoren ondernemers aanzetten tot actie. Uw input helpt om dit beter in kaart te brengen.

Het invullen van de vragenlijst duurt ongeveer 10 minuten.

Uw deelname is volledig anoniem. De gegevens worden uitsluitend gebruikt voor academische doeleinden en zijn niet te herleiden tot individuele personen of bedrijven.

Onder de deelnemers worden twee bol.com cadeaukaarten t.w.v. €25 verloot als blijk van waardering voor uw deelname.

Aan het einde van de vragenlijst kunt u – indien gewenst – uw e-mailadres opgeven om mee te doen aan deze winactie. Dit e-mailadres wordt losgekoppeld van uw antwoorden verwerkt.

Uw medewerking is van grote waarde voor het slagen van dit onderzoek. Hartelijk dank voor uw tijd en bijdrage!

De survey begint op de volgende pagina. Als je vragen of opmerkingen hebt, kun je contact opnemen met de onderzoeker, Max Masselink, via max.masselink@ru.nl. Nogmaals hartelijk dank voor uw deelname.

De retail sector houdt zich bezig met de verkoop van goederen en diensten aan consumenten, zowel via fysieke winkels als online kanalen.

Valt uw onderneming binnen de retailsector?

- Ja
- Nee

Waar is uw onderneming gevestigd?
(Indien uw onderneming in meerdere provinicies is gevestigd dan kan u meerdere antwoorden selecteren.)

- Drenthe
- Flevoland
- Friesland
- Gelderland
- Groningen
- Limburg
- Noord-Brabant
- Noord-Holland
- Overijssel
- Utrecht
- Zeeland
- Zuid-Holland
- Buiten Nederland

Categorie	Netto-omzet (€)	Balanstotaal (€)	Aantal werknemers (FTE)
A.	0 – 900.000	0 – 450.000	0 – 10
B.	900.001 – 15.000.000	450.001 – 7.500.000	11 – 50
C.	15.000.001 – 50.000.000	7.500.001 – 25.000.000	51 – 250
D.	> 50.000.000	> 25.000.000	> 250

Om de juiste categorie van uw onderneming te bepalen, kijken we in dit onderzoek naar de omvang van uw bedrijf. Die omvang wordt vastgesteld aan de hand van drie criteria:
1. Netto-omzet: Dit is het geld dat uw bedrijf heeft verdiend met verkopen, zonder btw en kortingen.
2. Balanstotaal: Dit is de totale waarde van alles wat uw bedrijf bezit en schuldig is.
3. Aantal werknemers (FTE): Dit is het aantal mensen dat fulltime bij uw bedrijf werkt, inclusief deeltijders omgerekend naar hele banen.
Er zijn vier categorieën (A, B, C en D). Uw onderneming valt in een bepaalde categorie als zij aan minstens twee van de drie bovenstaande criteria voldoet.

Tot welke categorie behoorde uw onderneming in het **afgelopen boekjaar**?
Let op: Uw onderneming valt in een bepaalde categorie als zij aan minstens twee van de drie

bovenstaande criteria voldoet.

(U kunt een schatting geven als u de exacte cijfers niet weet.)

- Categorie A
- Categorie B
- Categorie C
- Categorie D
- Uw onderneming voldoet niet aan ten minste twee van de drie criteria voor één van de vier categorieën.

Tot welke categorie behoorde uw onderneming **twee boekjaren geleden**?

Let op: Uw onderneming valt in een bepaalde categorie als zij aan minstens twee van de drie bovenstaande criteria voldoet.

(U kunt een schatting geven als u de exacte cijfers niet weet.)

- Categorie A
- Categorie B
- Categorie C
- Categorie D
- Uw onderneming voldoet niet aan ten minste twee van de drie criteria voor één van de vier categorieën.

Control variables:

Wat is uw functie binnen de organisatie?

- Eigenaar / Directeur
- IT-manager / ICT-verantwoordelijke
- Financieel verantwoordelijke
- Administratief medewerker
- Medewerker verkoop / winkelvloer
- Anders, namelijk: _____

Wat is uw leeftijd?

- Jonger dan 25 jaar
- 25–34 jaar
- 35–44 jaar
- 45–54 jaar
- 55–64 jaar
- 65 jaar of ouder

Wat is uw geslacht:

- Man
- Vrouw
- Wil ik niet zeggen
- Anders, namelijk: _____

Maakt uw organisatie gebruik van digitale systemen voor kernactiviteiten (zoals voorraadbeheer, klantcommunicatie of betalingen)?

- Ja, voor meerdere kernactiviteiten
- Ja, voor enkele kernactiviteiten
- Nee
- Weet ik niet

Heeft uw organisatie een medewerker of externe partij verantwoordelijk voor IT of cybersecurity?

- Ja, een interne medewerker
- Ja, een externe dienstverlener
- Ja, zowel intern als extern
- Nee, niemand is hier specifiek voor verantwoordelijk
- Weet ik niet

Via welk(e) kanaal/kanalen is uw onderneming voornamelijk actief in het contact met klanten en/of de verkoop van producten of diensten?

- Enkel fysiek (bijvoorbeeld via winkels, beurzen of kantoorlocaties)
- Enkel online (bijvoorbeeld via een webshop, app of platform)
- Zowel fysiek als online
- Anders, namelijk: _____

For all statements below:

(1) Strongly disagree (5) Somewhat agree
(2) Disagree (6) Agree
(3) Somewhat disagree (7) Strongly agree
(4) Neutral (8) Do not know / No opinion

Geef aan in hoeverre de onderstaande uitspraken van toepassing zijn op u of op uw organisatie.

RBV:

Onze investeringen in cybersecurity zorgen zichtbaar voor betere prestaties of minder risico's binnen ons bedrijf. (1) (2) (3) (4) (5) (6) (7) (8)

De manier waarop onze mensen, processen en technologie samenkomen op het gebied van cybersecurity is uniek. (1) (2) (3) (4) (5) (6) (7) (8)

Bij ons wordt cybersecurity gezien als een belangrijk strategisch hulpmiddel, en niet alleen als een IT-kost of verplichting. (1) (2) (3) (4) (5) (6) (7) (8)

PMT:

Een cyberaanval op ons bedrijf zou grote gevolgen kunnen hebben.

(1) (2) (3) (4) (5) (6) (7) (8)

Ik geloof dat cybersecuritymaatregelen ons bedrijf goed kunnen beschermen tegen digitale dreigingen. (1) (2) (3) (4) (5) (6) (7) (8)

Ik ben van plan om ons bedrijf actief te beschermen tegen cyberdreigingen.

(1) (2) (3) (4) (5) (6) (7) (8)

PU:

Cybersecuritymaatregelen helpen mij om grip te houden op belangrijke processen in mijn bedrijf

(1) (2) (3) (4) (5) (6) (7) (8)

Door cybersecuritymaatregelen kan ik sneller en beter handelen als er iets misgaat zoals bij een digitale aanval. (1) (2) (3) (4) (5) (6) (7) (8)

Cybersecurity helpt mee om mijn bedrijf draaiende te houden ook in moeilijke situaties.

(1) (2) (3) (4) (5) (6) (7) (8)

Dankzij goede cyberbeveiliging werk ik met een veiliger en geruster gevoel.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecuritytools zijn nuttig om risico's binnen mijn bedrijf goed te beheren.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecurity helpt mij om betere beslissingen te nemen omdat ik over meer en betere informatie beschik. (1) (2) (3) (4) (5) (6) (7) (8)

Cybersecuritytools zorgen ervoor dat mijn digitale processen soepeler en beter verlopen.

(1) (2) (3) (4) (5) (6) (7) (8)

Door cybersecurity wordt de kwaliteit van hoe ik mijn bedrijf run verbeterd.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecuritymaatregelen geven me meer controle over mijn dagelijkse werkzaamheden.

(1) (2) (3) (4) (5) (6) (7) (8)

Door cybersecuritymaatregelen kan ik mijn taken sneller afronden.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecurity ondersteunt belangrijke onderdelen van mijn werk.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecuritymaatregelen maken mijn werk effectiever.

(1) (2) (3) (4) (5) (6) (7) (8)

Door goede cybersecurity kan ik beter presteren in mijn werk.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecurity maakt het makkelijker om mijn werk goed te doen.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecuritymaatregelen zijn nuttig voor het dagelijks runnen van mijn bedrijf.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecuritymaatregelen zorgen ervoor dat ik productiever ben.

(1) (2) (3) (4) (5) (6) (7) (8)

PEoU:

Het is voor mij of mijn bedrijf makkelijk om cybersecuritymaatregelen in te voeren.

(1) (2) (3) (4) (5) (6) (7) (8)

Ik voel me op mijn gemak met de tools of richtlijnen die te maken hebben met cyberveiligheid.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecuritymaatregelen zijn flexibel en passen zich goed aan aan wat we nodig hebben.

(1) (2) (3) (4) (5) (6) (7) (8)

Ik kan makkelijk doen wat ik wil met de beschikbare beveiligingsmaatregelen.

(1) (2) (3) (4) (5) (6) (7) (8)

Het uitvoeren van beveiligingstaken is eenvoudig met de cybersecuritymaatregelen die we gebruiken. (1) (2) (3) (4) (5) (6) (7) (8)

Ik vind cybersecuritymaatregelen vaak ingewikkeld om te gebruiken.

(1) (2) (3) (4) (5) (6) (7) (8)

Het werken met cybersecuritymaatregelen is soms frustrerend.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecuritymaatregelen zijn vaak niet flexibel en moeilijk aan te passen aan onze werkwijze.

(1) (2) (3) (4) (5) (6) (7) (8)

Het kost me veel moeite en concentratie om goed om te gaan met cybersecuritymaatregelen.

(1) (2) (3) (4) (5) (6) (7) (8)

Het kost veel tijd en moeite om goed te leren omgaan met cybersecuritymaatregelen.

(1) (2) (3) (4) (5) (6) (7) (8)

Ik hoef er niet veel over na te denken om cybersecuritymaatregelen te gebruiken.

(1) (2) (3) (4) (5) (6) (7) (8)

Ik hoef er niet veel over na te denken om cybersecuritymaatregelen te gebruiken.

(1) (2) (3) (4) (5) (6) (7) (8)

De regels en stappen rond cyberbeveiliging zijn duidelijk en goed te begrijpen.

(1) (2) (3) (4) (5) (6) (7) (8)

Het is makkelijk om cybersecuritymaatregelen goed toe te passen in mijn bedrijf.

(1) (2) (3) (4) (5) (6) (7) (8)

Het navigeren of rondkijken in cybersecuritytools gaat gemakkelijk.

(1) (2) (3) (4) (5) (6) (7) (8)

Ik onthoud gemakkelijk hoe ik beveiligingstaken moet uitvoeren.

(1) (2) (3) (4) (5) (6) (7) (8)

Cybersecuritymaatregelen zijn over het algemeen makkelijk in gebruik.

(1) (2) (3) (4) (5) (6) (7) (8)

NIST:

Wij hebben een duidelijk en actueel overzicht van alle IT-systemen, software en apparaten die binnen ons bedrijf worden gebruikt.

(1) (2) (3) (4) (5) (6) (7) (8)

Wij weten precies welke digitale gegevens en systemen het belangrijkst zijn om onze bedrijfsvoering draaiende te houden.

(1) (2) (3) (4) (5) (6) (7) (8)

Het afgelopen jaar is er op een serieuze en gestructureerde manier onderzocht welke risico's wij lopen op het gebied van cyberveiligheid, en de resultaten daarvan zijn vastgelegd.

(1) (2) (3) (4) (5) (6) (7) (8)

Onze medewerkers krijgen regelmatig uitleg of training over veilig online gedrag en cyberveiligheid. (1) (2) (3) (4) (5) (6) (7) (8)

Alle apparaten en accounts in ons bedrijf zijn goed beveiligd met sterke wachtwoorden en/of tweestapsverificatie (bijvoorbeeld een extra code via sms of e-mail).

(1) (2) (3) (4) (5) (6) (7) (8)

Alle apparaten en accounts in ons bedrijf zijn goed beveiligd met sterke wachtwoorden en/of tweestapsverificatie (bijvoorbeeld een extra code via sms of e-mail).

(1) (2) (3) (4) (5) (6) (7) (8)

We maken regelmatig back-ups van belangrijke gegevens en controleren of deze back-ups ook echt werken. (1) (2) (3) (4) (5) (6) (7) (8)

We gebruiken antivirussoftware en firewalls en die worden regelmatig bijgewerkt.

(1) (2) (3) (4) (5) (6) (7) (8)

Wij gebruiken software of tools om te kunnen zien als er iets opvallends of verdachts gebeurt op ons computernetwerk. (1) (2) (3) (4) (5) (6) (7) (8)

Binnen ons bedrijf is duidelijk wat je moet doen als iemand iets verdachts opmerkt, zoals een verdachte e-mail of inbraakpoging.

(1) (2) (3) (4) (5) (6) (7) (8)

Ons bedrijf heeft een duidelijk stappenplan klaarliggen voor als we te maken krijgen met een cyberaanval of ander digitaal incident.

(1) (2) (3) (4) (5) (6) (7) (8)

Onze medewerkers weten wat ze moeten doen als er een cyberincident gebeurt (zoals een hack of datalek). (1) (2) (3) (4) (5) (6) (7) (8)

Als we eerder een cyberincident hebben gehad, kijken we achteraf wat er goed en fout ging om het de volgende keer beter aan te pakken.

(1) (2) (3) (4) (5) (6) (7) (8)

Wij hebben een herstelplan dat bepaalt hoe systemen worden teruggezet na een aanval.

(1) (2) (3) (4) (5) (6) (7) (8)

Ons bedrijf heeft geïnvesteerd in maatregelen om snel te kunnen herstellen van een cyberaanval.

(1) (2) (3) (4) (5) (6) (7) (8)

Voucher raffle

Wilt u na het invullen van deze survey deelnemen aan de winactie voor een Bol.com cadeau kaart?

De winnaar wordt benaderd per mail. Laat daarom hieronder uw e-mail achter.

Wanneer u hier uw e-mail achter laat wordt deze uitsluitend gebruikt voor de winactie.

- Nee
- Ja, mijn e-mail is: _____

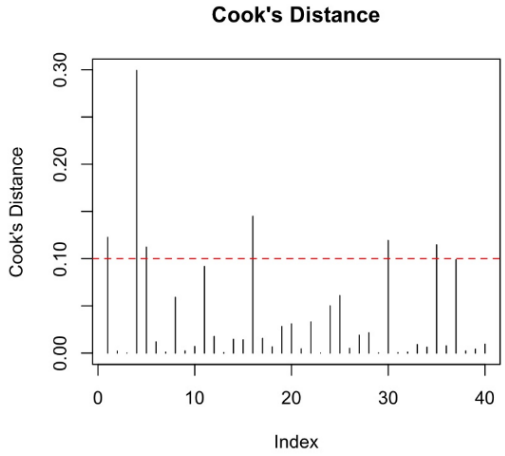
Closure

We thank you for your time spent taking this survey.

Your response has been recorded.

7.2 Cook's distance analysis

Figure 3: Cook's Distance-analyse



The graph shows that several observations have a Cook's Distance above the red threshold line, indicating a relatively large influence of these points on the regression model. Visually, it appears that there are six observations above this threshold, but in reality there are eight: namely, observations 1, 4, 5, 16, 30, 31, 35 and 36.

7.3 Power-analyse

Table 10: Power-analyse

Power-analyse
u = 8
v = 31
f2 = 0.15
sig.level = 0.05
power = 0.2826381

7.4 Generative artificial intelligence

Generative artificial intelligence was used in the development of the text for this research. However, the input and all information were not created and/or found by the generative artificial intelligence. The only purposes for which the generative AI was used were to rewrite text and to code. The generative AI tool used was ChatGPT, which was developed and is maintained by the American company OpenAI. This website can be found at the following link: https://openai.com/chatgpt/overview/.

While all AI-generated output was initially reviewed to ensure it aligned with the original input, it is possible that certain sections were later modified or supplemented manually. As a result, some of the final content may not be traceable to the original inputs listed below.
The same prompt was used for all the inputs below, namely:
"Herschrijf dit naar wetenschappelijker taal gebruik. Zorg er voor dat de inhoud hetzelfde blijft en ook dat het brongebruik hetzelfde blijft. Doe dit in het Engels. Zorg dat de boodschap dus hetzelfde is."
In English, this prompt is:
"Rewrite this to more scientific language usage. Make sure the content remains the same and also that the source usage remains the same. Do this in English. So make sure the message is the same."
All output generated by ChatGPT was critically reviewed, verified, and, where necessary, adjusted to ensure consistency with the original text, which can be found below.

Inputs:

Input: Small and medium-sized enterprises (SMEs) are an important part of the economy, but they often struggle with cybersecurity. Even though there's growing attention from policymakers, many SMEs lack the resources and support needed to handle cyber threats properly. As noted by Chidukwani, Zander, and Koutsakis (2022), most cybersecurity research focuses on large companies, while studies on SMEs are usually qualitative and mainly look at risk assessment and prevention. Key areas like detection, response, and recovery are still not explored enough.
Within the SME sector, retail stands out as especially relevant. In recent years, the retail industry has gone through a digital transformation, making businesses more dependent on information systems for daily operations, customer communication, and data management. This shift has also made them more vulnerable to cyber risks (Vaka, 2025). Besides being economically important—by creating value in the supply chain and offering opportunities for entrepreneurs—retail SMEs face serious cybersecurity challenges (Levy & Grewal, 2023). Many of these businesses have limited cyber resilience and don't always see cybercrime as a major risk. Nearly half of the companies surveyed reported experiencing a cyber incident in the past year, and 12% suffered financial or operational damage. (Van der Kleij et al., 2019)

This paper looks at how cybersecurity awareness influences cybersecurity investments among Dutch SMEs in the retail sector.

Input: According to research by Thales (2022), 45% of retailers have seen an increase in both how often and how seriously they're being hit by cyberattacks. On top of that, 52% report more incidents of e-commerce fraud (National Retail Federation, 2023). These trends show that the threat level in the retail sector is growing, especially as the industry becomes more dependent on digital systems.

As physical and online sales channels continue to merge, new security gaps are appearing. Organised Retail Crime (ORC) is no longer just about shoplifting in physical stores—it's increasingly shifting to digital environments, using more sophisticated methods (National Retail Federation, 2023).

Even though awareness of cyber risks is growing, many retailers still struggle to deal with them effectively. Often, their cybersecurity efforts are reactive instead of strategic. This is usually because of limited resources and uncertainty about what the right steps are. That's why it's important to have both technical and organisational safeguards in place. Working with specialiced cybersecurity providers can also help tackle these challenges. (Symantec)

Because everything in the digital world is so interconnected, poor cybersecurity doesn't just affect individual businesses. It can also disrupt critical systems and services and reduce public trust in digital technology (Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2022; 2023).

Input: The Cyber Security Council (CSR) recommends a more practical and focused strategy to improve the cyber resilience of SMEs. Their suggestions include setting up a one-stop helpdesk within the National Cyber Security Centre (NCSC), encouraging public-private partnerships, and developing standardised solutions backed by an official quality label (Cyber Security Raad, 2024).

Heidt, Gerlach, and Buxmann (2019) looked into the differences in IT security investments between SMEs and large companies. They argue that many existing studies don't take the situation of SMEs into account. Based on a review of the literature and interviews with 25 experts, they identified several SME-specific factors that influence IT security decisions. Their findings show that assumptions often made in the literature—like having trained staff or formal processes—don't always hold true for smaller businesses. While the study offers useful insights into the structural challenges SMEs face when investing in IT security, it doesn't directly look at how cybersecurity awareness influences those investment choices (Heidt, Gerlach, & Buxmann, 2019).

Input: Chidukwani, Zander, and Koutsakis (2022) point out that there's still very little research on how SMEs deal with detecting, responding to, and recovering from cyber threats. They call for more data-driven studies in these areas. Even though this is an important topic, we still don't know much about how cybersecurity awareness actually affects investment decisions within SMEs. That's a concern, especially since many people still have limited knowledge of information security, and overall awareness remains low (Al-Janabi, 2016).

Technology alone isn't enough to handle all security threats, especially with the increasing complexity of today's digital risks. That's why it's crucial for users to be aware and have the right skills to protect themselves (Furnell & Clarke, 2012).

The gap between awareness and actual investment is also visible in the data. According to the Dutch Central Bureau of Statistics (2024), larger companies are more likely to implement cybersecurity measures than smaller ones. On top of that, the Nationaal Coördinator Terrorismebestrijding en Veiligheid (2021) warns that SMEs often don't have the knowledge or money to boost their cybersecurity, even though they're frequent targets for cybercriminals.

This study adds to existing research by exploring how cybersecurity awareness impacts investment in security measures, specifically among Dutch SMEs in the retail sector.

Input: This research offers practical insights into how cybersecurity awareness is linked to investment behaviour in SMEs. The findings can help policymakers evaluate how effective current awareness campaigns really are, and whether these efforts need to be adjusted to better encourage businesses to invest in security.

To strengthen cybersecurity across society, the Dutch government has launched several initiatives aimed at improving the "human factor" in cyber defence. These include awareness campaigns, podcasts, online tools, and webinars—all funded with public money (Digitale Overheid, 2025). While these efforts aim to boost awareness, it's still unclear whether they actually lead to changes in behaviour or more investments in cybersecurity. That's why it's important to look at whether these campaigns really encourage SMEs to take concrete action. If public resources are used more effectively, they could help boost society's overall resilience against cyber threats.

The NIS2 Directive is designed to improve cybersecurity by introducing stricter rules, expanding regulations, encouraging collaboration with Computer Security Incident Response Teams (CSIRTs), and promoting compliance with international standards (Ruohonemr, 2024). CSIRTs are specialised teams that detect, analyse, and coordinate responses to cyber incidents within and

across organisations. According to Rijksdienst voor Ondernemend Nederland (2025), the directive mainly applies to medium and large organisations in critical or very critical sectors. That means SMEs in the retail sector aren't legally required to take cybersecurity measures. This regulatory gap provides a useful backdrop for this study, as it allows us to explore whether awareness campaigns and communication efforts, without any legal pressure, can still lead SMEs to invest in cybersecurity. If awareness alone drives action, that insight can help shape better policy in the future.

At the same time, European regulations are having an indirect impact on how SMEs handle cybersecurity. The updated NIS2 Directive places requirements on key organisations to take proper security steps and report incidents. Likewise, the upcoming Cyber Resilience Act (CRA) sets standards for the security of digital products and services. While many SMEs aren't directly affected by these laws, they're increasingly feeling the pressure through supply chain demands and higher expectations from bigger clients and partners (Cyber Security Raad, 2024).

By exploring the connection between cybersecurity awareness and investment behaviour in SME retailers, this study helps clarify how current policies and campaigns are influencing real-world security practices in smaller businesses.

Input: "In cybersecurity, it's widely accepted that one digital system's strength depends on the strength of others. The overall safety of the digital world relies heavily on the weakest links" (Cobos, 2024, p. 80). Since SMEs are often among the most vulnerable, weak protection on their side can seriously affect the digital resilience of society as a whole. "Cyber risk is a textbook example of a systemic risk. Exposures to cyber risk are common across firms, and risks become highly correlated under stress" (Kopp, Wilson, & Kaffenberger, 2017, p. 7). In other words, when something goes wrong, the problems can quickly spread and affect the stability of the entire system. Systemic cyber risk happens when a cyberattack on one part of a critical infrastructure sets off a chain reaction, disrupting other areas. This can damage service delivery, compromise data, and even threaten economic, societal, or national security (World Economic Forum, 2016). It shows how interconnected everything is, if one link in the supply chain is weak, it can affect everyone else. A cyberattack on a supplier, for example, could give hackers a way into your own systems and your customers' systems too (Nationaal Cyber Security Centrum, 2023).

Regulatory Context: The NIS2 Directive

The NIS2 Directive lays out strict cybersecurity rules for medium and large companies operating

in critical sectors. It requires them to boost their security measures, report cyber incidents, and follow national strategies to strengthen resilience. It's up to each EU country to monitor whether companies comply and to issue penalties if they don't. Meanwhile, the EU promotes cooperation and information sharing across member states (European Commission, 2022). However, this directive doesn't apply to the retail sector (Rijksdienst voor Ondernemend Nederland, 2025).

Research Question and Objectives

Because there's no specific cybersecurity law for retail-sector SMEs, these businesses don't always see cybersecurity as a top priority. Still, the government invests heavily in awareness campaigns—paid for with public funds—that are meant to encourage individuals and businesses to take action. Yet research shows that even though awareness of cyber risks is growing among retailers, this hasn't resulted in a major push to implement stronger security measures.

Input: Cybersecurity investments in practice can be both technical and organisational. Technical investments include implementing firewalls, anti-virus software, backup systems and multi-factor authentication. Organisational investments, on the other hand, include creating an information security policy, training staff and engaging external expertise (Chidukwani, Zander, & Koutsakis, 2022; Jamil, Zia, Nayeem, Whitty, & Alessandro, 2025). This broad interpretation is in line with previous studies analysing cybersecurity investments based on the quantity, variety and degree of implementation of security measures, rather than exact financial amounts (Rombaldo, Becker, & Johnson, 2023; Zwilling, Wiechetek, Lesjak, & Çetin, 2022). This puts the emphasis on the depth and applicability of practical security actions within organisations.

Input: Investments in cybersecurity can be both technical - such as the implementation of firewalls, antivirus software, backups and multifactor authentication - and organisational, such as the creation of an information security policy, training staff or hiring external experts (Chidukwani, Zander, & Koutsakis, 2022) (Jamil, Zia, Nayeem, Whitty, & Alessandro, 2025). This broad interpretation is in line with previous studies that analyse cybersecurity investments based on the quantity, variety and degree of implementation of security measures, rather than exact financial amounts (Rombaldo, Becker, & Johnson, 2023; Zwilling, Wiechetek, Lesjak, & Çetin, 2022). Both studies adopt a broader interpretation of investment behaviour, focusing on the practical implementation and depth of security measures within organisations or among individual employees.

Input: The original Technology Acceptance Model (Davis, 1987) focuses on technology acceptance and explains behaviour using two main constructs: perceived usefulness (PU) and perceived ease of use (PEoU). Both have been empirically validated as reliable predictors of behavioural intention regarding technological innovations (Holden & Karsh, 2010).
In the context of cybersecurity, these variables can be interpreted as the expected contribution of cybersecurity measures to business continuity (PU), and the perceived ease of implementation (PEoU), respectively. Alsmadi (2024) shows that perceptions about threat and complexity directly affect these two constructs. His study confirms that PU and PEoU are also important factors within cybersecurity contexts that determine whether entrepreneurs are willing to accept and implement measures.

Input: Cybersecurity awareness refers to the extent to which individuals within an organisation are aware of cyber threats, their potential consequences, and the measures available to mitigate risks. In the context of SMEs, awareness is particularly important because many companies have limited resources and human actions are often the weakest link in the security chain (Furnell & Clarke, 2012; Jamil, Zia, Nayeem, Whitty, & Alessandro, 2025).
This approach is in line with previous research measuring cybersecurity awareness through self-report, focusing on three components: knowledge, perception of threat, and behavioural intention (Shojaifar & Järvinen, 2021; Zwilling, Wiechetek, Lesjak, & Çetin, 2022).

Input: For this research, four core variables within PMT are important: threat severity (the severity of a cyber attack), threat vulnerability (the perceived likelihood of becoming a victim), response efficacy (the belief in the effectiveness of countermeasures) and self-efficacy (the confidence in one's own ability to successfully implement these measures) (Floyd, Prentice-Dunn, & Rogers, 2006).
Jamil et al (2025) applied this model to micro-entrepreneurs in Australia and found that these four components are strong predictors of cybersecurity behaviour. They also found that high response costs - such as expected time commitment or financial burden - negatively affect willingness to invest in cybersecurity. Protection Motivation Theory appears to be an effective framework to explain the cybersecurity behaviour of SMEs, especially when perceptions of threat and actionability are explicitly included in the analysis (Jamil, Zia, Nayeem, Whitty, & Alessandro,

2025).

Input: Besides this strategic approach, some studies adopt a broader interpretation of investment behaviour. Here, the focus is not on exact financial amounts, but on the quantity, variety and degree of implementation of security measures within an organisation (Rombaldo, Becker, & Johnson, 2023; Zwilling, Wiechetek, Lesjak, & Çetin, 2022). The focus is on the depth of practical security actions, both at the organisational level and among individual employees.

Input: Building on the understanding of cybersecurity training acceptance, it is relevant to examine whether cybersecurity awareness translates into concrete protective actions and investments within SMEs. A theoretical starting point of this research is the relationship between cyber awareness, knowledge and protection behaviour. Previous research shows that although internet users are aware of cyber threats, this awareness does not necessarily lead to concrete protection behaviour (Zwilling, Wiechetek, Lesjak, & Çetin, 2022). This study conducted in Israel, Slovenia, Poland and Turkey confirms that a higher level of cyber knowledge correlates with greater awareness and increased use of protective measures. However, this does not necessarily result in a decreased willingness to share personal, and thus sensitive, information (Zwilling, Wiechetek, Lesjak, & Çetin, 2022). This indicates a difference between awareness and actual behaviour, suggesting that technological solutions alone are not sufficient. Effective protection also requires the presence of appropriate knowledge and skills among users, these are important in addition to technological solutions (Furnell & Clarke, 2012). Cybersecurity awareness refers to the extent to which individuals within an organisation recognise cyber threats, understand their potential impact, and are informed about measures to mitigate associated risks. Within the context of small and medium-sized enterprises (SMEs), this awareness is particularly relevant, as such organisations often operate with limited resources, and human behaviour can represent a significant vulnerability in the security framework (Furnell & Clarke, 2012; Jamil, Zia, Nayeem, Whitty, & Alessandro, 2025). This perspective aligns with earlier studies that assess cybersecurity awareness through self-reported data, typically focusing on three dimensions: knowledge, perceived threat, and behavioural intention (Shojaifar & Järvinen, 2021; Zwilling, Wiechetek, Lesjak, & Çetin, 2022). The study by Zwilling et al. (2022) suggests that cyber awareness and protection behaviour differ by country, with higher levels in economically developed countries. According to the (Cyber

Security Raad, 2024), limited cyber awareness and investment uncertainty increases the risk of cyber incidents within Dutch SMEs. This research builds on this by analysing how cyber security awareness affects SME investment and whether there are sectoral differences.

Input: The NIST Cybersecurity Framework (NIST, 2018) provides a flexible, cross-sectoral framework that allows organisations to identify, manage and reduce their cyber risks using five core tasks (Identify, Protect, Detect, Respond, Recover), complemented by Implementation Tiers and Framework Profiles for maturity assessment and risk prioritisation. Jamil et al. (2025) highlight the relevance of this framework for small businesses, noting that adoption rates remain low despite the availability of simplified guidelines (such as NISTIR 7621); small businesses score low on average across all NIST domains, indicating limited cyber maturity. Moore et al (2015) show that cybersecurity frameworks such as the NIST framework are widely used within organisations as a tool to structure investment decisions and translate from technical risks to business priorities. Within government organisations is strong influence of slow budget cycles and regulations (Moore). This study applies the NIST Framework to analyse the extent to which Dutch SME retailers invest in cybersecurity measures.

Input: One framework that fleshes out this broad approach to cybersecurity investments is the NIST Cybersecurity Framework. The NIST Cybersecurity Framework aligns with the literature described earlier in which cybersecurity investments are approached as a combination of technical and organisational measures aimed at practical implementation and mitigation of economic risks within organisations.

Input: This study uses a quantitative, cross-sectional, survey research to investigate the relationship between cyber security awareness and investment in cyber security measures among Dutch SME retailers. The reason for choosing a cross-sectional survey, measuring at one point in time, is because of lack of time and resources to measure at more points in time. The survey approach was chosen because this method allows for targeted data collection on cybersecurity investments and awareness among SME retailers, a target group for which such information is usually not publicly available. Publicly available data on cybersecurity in SMEs are limited (Chidukwani et al., 2022; Rombaldo et al., 2023).

Participation of individuals in this project is voluntary. This research used a web-based online survey instrument designed using Qualtrics. The survey will be developed using existing conceptual framework and will incorporate elements from established theoretical models to support content validity. The models used for this purpose are TAM, CTAM, PMT and RBV. This approach is consistent with previous survey-based research aimed at exploring patterns and relationships in current organisational contexts.

Input: Perceived Usefulness (PU) and Perceived Ease of Use (PEoU) are included as measurement tools in the survey, to identify the cognitive drivers behind investment readiness (Davis, 1989; Holden & Karsh, 2010; Alsmadi, 2024). This identifies the extent to which SME entrepreneurs expect data insights to help them make effective cybersecurity investment decisions and the extent to which they perceive the use of data insights as easy and accessible. The survey items gauge the extent to which respondents expect cybersecurity measures to contribute to their business continuity, as well as their perception of the user-friendliness of these measures.
This aims to better understand the psychological components underlying investment behaviour, complementing the more risk-oriented approach from PMT.

Input: By including CTAM variables in the survey, psychological and contextual barriers to investment behaviour can be identified (Fallatah, Kävrestad & Furnell, 2024; Nurqamarani et al., 2021). Survey items will gauge, among other things, feelings of concern about cyber threats, confidence in available solutions, perceived indifference and the pressure felt from external parties such as legislators or supply chain partners. These factors offer additional explanatory power alongside the more cognitive and technological constructs from PMT and TAM, and contribute to a more complete picture of decision-making around cybersecurity investments

Input: Protection Motivation Theory (Floyd, Prentice-Dunn and Rogers, 2000) provides four core constructs - threat severity, threat vulnerability, response efficacy and self-efficacy - that can be effectively deployed to explain protective behaviour in a cybersecurity context. The PMT constructs thus provide a solid basis for measuring cybersecurity awareness in the survey. The questionnaire therefore contains items that measure the four core components. By including these

theoretically based variables, the validity of the awareness measurement is strengthened and a nuanced relationship can be established between awareness and investment behaviour.

Input: The Resource-Based View (RBV) shows that organisations invest in cybersecurity only when they view these capabilities as valuable and strategic assets that contribute to sustainable competitive advantage (Wernerfelt, 1984; Barney, 1991; Weishäupl et al., 2015; Rombaldo et al., 2023). These insights make it clear that it is important for the survey to measure the extent to which SMEs view cybersecurity as a strategic asset, and whether they have the necessary resources to invest in it. Survey items will focus on the presence of staff, IT infrastructure, internal policies and strategic priority of cybersecurity. By including these aspects, it will be possible to examine whether limited resources or low priority are a barrier to investing in digital resilience, in line with the RBV perspective

Input: The dependent variable in this study is the level of investment in cybersecurity measures within Dutch SME retailers. This variable is measured using a composite index score based on survey questions that specifically assess the extent to which an organisation has implemented concrete cybersecurity measures. The construction of these questions is inspired by the NIST Cybersecurity Framework, which consists of five core functions (Identify, Protect, Detect, Respond, Recover) and 22 associated categories with a total of 98 subcategories (Almuhammadi & Alsaleh, 2017; Scofield, 2016). Jamil et al (2025) also emphasise the importance of the NIST Framework as a guide for structuring and measuring cybersecurity practices within small businesses. Each survey question which the dependent variable wants to measure links to one or more subcategories and thus measures whether the organisation uses certain investments. Respondents indicate the extent to which each measure is applied (e.g. not, partially or fully). Based on this, a continuous index score is calculated, counting both the number and type of measures. This measurement method allows quantitative comparison of the level of investment and is in line with existing field studies such as Moore et al. (2015) and Jamil et al. (2025), where cybersecurity is seen not purely financial, but as a strategic choice process.

Input: The independent variable in this study is cybersecurity awareness. It is defined as ‘the knowledge and overall understanding of information-security-related problems and their

repercussions as well as what needs to be done to handle them' (Khan, Ikram, & Saleem, 2023, p. 2). The data related to this variable is collected using a survey, composed of survey items that gauge knowledge of risks, attitudes towards cybersecurity and level of familiarity with concrete security practices. The underlying factors measured are drawn from four theoretical models: Protection Motivation Theory (PMT), the Technology Acceptance Model (TAM), the Cybersecurity Training Acceptance Model (CTAM) and the Resource-Based View (RBV). These factors are shown schematically in the table below:

Input: The model of Haeussinger and Kranz (2013) provides an empirically based framework that explains how Information Security Awareness (ISA) is established and its role in explaining employees' intention to comply with security policies (Haeussinger & Kranz, 2013). Within this model, ISA is defined from a cognitive approach, as a state of awareness and knowledge about information security goals, risks and threats, and an interest in acquiring the necessary knowledge to act information responsibly (Haeussinger & Kranz, 2013). The authors identify several determinants of ISA, including knowledge about information systems and actively providing clear, understandable and available information security policies, as the most influential (Haeussinger & Kranz, 2013). In addition, they show that security training, information from secondary sources (such as media) and the behaviour of colleagues also contribute to the level of ISA (Haeussinger & Kranz, 2013). In their model is the role of ISA as a mediating variable: ISA mediates the relationship between these influencing factors and employees' intention to comply with security policies (Haeussinger & Kranz, 2013). In doing so, the authors find empirical evidence for a direct, positive relationship between ISA and compliance intention (Haeussinger & Kranz, 2013).

Input: Only 40 responses were usable for this study, which is quite a small sample. To check how reliable the regression results were, bootstrapping was used as an extra method. Bootstrapping is a statistical technique where you repeatedly draw random samples, with replacement, from the original data. This helps assess whether the effects you see are stable and consistent. In this case, the bootstrap was applied only to the key variables PU and PEoU. Including the full model with control variables didn't work well, some of the categorical variables didn't show up often enough in the resampled data, which caused errors or made the regressions fail to converge. That's why the decision was made to run the bootstrap analysis only on the simpler model, where PU and PEoU predict investment in cybersecurity. In total, 10,000 iterations were run to reduce the impact

of random variation (also known as Monte Carlo variation) and to get solid confidence intervals (Hesterberg, 2011). This approach gives a more reliable and realistic estimate of how strong the relationships in the basic model really are.

Input: In this study, Y_i stands for the level of cybersecurity investment made by firm i. This is measured using a composite index score based on the NIST Cybersecurity Framework. Awareness_i refers to the cybersecurity awareness level of firm i, calculated as the average of two key concepts from the Technology Acceptance Model (TAM): Perceived Usefulness (PU) and Perceived Ease of Use (PEoU). This score reflects how useful and easy firms think it is to work with cybersecurity tools and training. X_i is a set of control variables, including age, gender, digital maturity, whether the firm has an IT specialist, regional location, and other theoretical constructs such as PMT and RBV. Lastly, ε_i is the error term that captures any variation in investment levels that the model doesn't explain.

The goal of the model is to understand the general link between cybersecurity awareness and investment behaviour, specifically within the Dutch SME retail sector. Since the data were collected at a single point in time, the model doesn't include fixed effects or time trends.

To deal with possible heteroskedasticity and make sure the results are reliable, robust standard errors are used—following White's (1980) method. This approach adjusts for potential differences in variance between observations, which is especially relevant given how varied SMEs can be.

The coefficient β_1 is expected to be positive, in line with hypothesis 1, which states that higher awareness levels lead to more investment in cybersecurity measures.

Input: *Table 5* shows the correlations between all explanatory variables as part of a multicollinearity check. Most variables are only weakly to moderately correlated with each other, which suggests there's limited overlap in what they explain. The strongest correlation is between PU and PMT ($r = 0.73$), which is fairly high, but still below the commonly used threshold for problematic multicollinearity ($r > 0.80$). The correlation between PU and PEoU ($r = 0.55$), and between PEoU and Systems ($r = 0.41$), are also statistically significant, but still fall within acceptable limits. The positive link between PU and PEoU aligns with previous findings in the literature (Sohn & Kwon, 2019).

What stands out are the negative correlations between Gender and PU ($r = -0.28$), and between Gender and PEoU ($r = -0.50$), suggesting that there are different patterns based on gender. Even though none of the correlations exceed critical thresholds, it's important to consider what they

might mean for the regression results. The strong correlation between PU and PMT, and to a lesser extent between PU and PEoU, could reduce the individual significance of PU or PEoU when they're included together in the same regression model. This happens because their explanatory power overlaps, making it harder to statistically isolate the effect of each variable. So if PU or PEoU turn out to be non-significant in some models, that might be due to these underlying relationships between the variables.

Input: *Table 6* presents the results of the Variance Inflation Factor (VIF) test, which checks for potential multicollinearity between the independent variables. A VIF value below 5 is usually seen as acceptable and doesn't point to serious multicollinearity issues. In this case, the average VIF is 1.72, which is quite low and suggests that the explanatory variables don't show problematic overlap. PU (2.23), PEoU (2.34), and PMT (2.79) have the highest VIF values, but all stay well below the critical threshold.

It's not surprising these values are a bit higher, since there's a clear theoretical link: PU and PEoU are both key components of the same model (TAM), and PMT deals with similar ideas about threat and response. Because of this overlap in content, the standard errors for PU and PEoU go up when both are included in the same model, which can reduce their statistical significance. But that doesn't mean the variables aren't important—it just shows that part of their explanatory power is shared. The other variables, like age, gender, and IT responsibility, have VIF values close to 1, confirming that they don't have any problematic correlations.

All in all, the VIF test results suggest that multicollinearity is not a problem for the reliability of the regression outcomes.

Input: Table 7 looks at how PU and PEoU influence investment in cybersecurity, measured using the NIST score. In model (1), only PU is included as an explanatory variable. The coefficient is positive and highly significant ($\beta = 0.377$, $p < 0.001$), with a low standard error (0.118), suggesting that the estimate is quite precise. This points to a clear link: the more useful cybersecurity is perceived to be, the more a firm tends to invest in it.

Model (2) includes only PEoU. Again, the coefficient is positive and significant ($\beta = 0.411$, $p < 0.001$), with a slightly higher standard error (0.134), but still well within acceptable bounds. This means that ease of use also plays an important role in investment behaviour.

In model (3), both PU and PEoU are included at the same time. While the coefficients for both remain positive (PU = 0.260; PEoU = 0.268), neither is statistically significant, and the standard

errors increase (0.132 and 0.148, respectively). This is likely due to multicollinearity—PU and PEoU are conceptually linked and show a moderate correlation (as seen in the correlation matrix), which means their effects overlap. That shared variance reduces the precision of the estimates, making it harder to detect significant effects for each one individually. Still, the model's overall explanatory power stays solid.

The R^2 value goes up from 0.210 in model (1) and 0.198 in model (2) to 0.274 in model (3). Adjusted R^2 also rises from 0.189 to 0.235, which supports the idea that the combined model does a better job of explaining differences in investment levels. So, even if the individual effects are less clear in model (3), the joint impact of PU and PEoU still shows a strong and consistent connection with cybersecurity investment.

Input: Table 8 presents the results of a bootstrap analysis for PU and PEoU, aimed at testing how robust their estimated effects are on the intention to invest in cybersecurity. For PU, the average coefficient is 0.272 (SD = 0.150), with a 95% confidence interval ranging from -0.036 to 0.552. For PEoU, the average is 0.293 (SD = 0.167), with a confidence interval from -0.016 to 0.647. While both variables show a positive effect, their confidence intervals include zero. This means the results aren't statistically significant, and we can't draw firm conclusions about the individual impact of PU or PEoU on investment behaviour based on this analysis.

One likely reason for the lack of significance is the small sample size, along with the overlapping explanatory power of PU and PEoU. These two are conceptually linked and show empirical correlation, which makes it harder to tease apart their separate effects. Bootstrap confidence intervals also tend to be broader, especially with smaller samples, so they're more likely to cross zero, even when the data hint at an effect. Despite this, the direction and magnitude of the coefficients suggest that both PU and PEoU might play a role in shaping investment intentions. Still, larger samples would be needed to confirm this more definitively.

Input: Table 9 looks at the effect of PU, PEoU, and awareness on cybersecurity investment (measured using the NIST score), this time including control variables. In model (1), where only PU is included, the coefficient is positive ($\beta = 0.288$), but not statistically significant. The standard error is 0.182, suggesting the estimate isn't very precise. So while PU seems to have a positive effect, this model doesn't provide strong evidence for it.

Model (2) includes only PEoU. Here too, the effect is positive (β = 0.317) but not significant, with a standard error of 0.211. This means PEoU alone doesn't explain much once control variables are included.

In model (3), both PU and PEoU are added together. Their coefficients remain positive (PU = 0.246; PEoU = 0.266), but still aren't statistically significant. The standard errors go up a bit (0.184 and 0.212), which could be due to multicollinearity—PU and PEoU are conceptually and empirically connected, so their effects might overlap. That overlap makes it harder to isolate each variable's individual influence, reducing their significance.

Model (4) introduces an interaction term (PU_PEoU) to see if PU and PEoU have a combined effect. This interaction is statistically significant (β = 0.255, $p < 0.05$) with a standard error of 0.124. This suggests that the joint influence of PU and PEoU matters—perhaps because their combined impact becomes clear only when looked at together.

Model (5) uses a composite variable called 'Awareness', calculated as the average of PU and PEoU. This fits with the Technology Acceptance Model, where both together shape behavioural intention. The coefficient here is significantly positive (β = 0.509, $p < 0.05$), with a standard error of 0.247. This means that firms with higher cybersecurity awareness are more likely to invest.

As for the control variables (like PMT, RBV, age, gender, IT responsibility, digital system use, and province), none of them are significant in any of the models. Their standard errors differ, but overall, they don't explain much. Still, the model's explanatory power improves: R^2 increases from 0.291 in model (1) to 0.327 in models (4) and (5), and adjusted R^2 goes up to 0.153. So even though not many variables are significant, the models perform better overall.

The main takeaway from Table 9 is that PU and PEoU don't show strong effects on their own—but when combined into a single awareness measure, or used together in an interaction term, their influence on investment readiness becomes significant. This is likely because PU and PEoU are strongly connected, and their combined effect is more stable and meaningful than their separate contributions.

Input: Table 10 presents a regression model that looks at the interaction between PU and PEoU in relation to cybersecurity investments, with control variables included. The goal of this model is to find out whether the combination of PU and PEoU has a reinforcing or weakening effect on firms' investment decisions.

Interestingly, both PU and PEoU on their own show negative coefficients (PU: $\beta = -0.375$; PEoU: $\beta = -0.469$), but neither is statistically significant. The standard errors are quite large (0.560 and 0.660), which indicates a lot of uncertainty in the estimates. This suggests that once the interaction term is added to the model, there's no strong evidence left for PU or PEoU having a separate effect. One reason for this could be multicollinearity: when variables are closely related, adding an interaction term can increase variance and make it harder to get precise estimates.

The interaction term PU*PEoU does show a positive coefficient ($\beta = 0.143$), but this effect isn't statistically significant either (standard error = 0.122). So while the direction of the effect suggests that combining PU and PEoU might boost investment in cybersecurity, the evidence is too weak to say so with confidence. A likely reason is again the small sample size, which may inflate the standard errors. Also, since PU and PEoU are conceptually closely linked, their shared variance could further complicate interpretation and reduce precision.

As for the control variables, none of them turn out to be significant in this model. Their coefficients are small and standard errors relatively high, which suggests they don't explain much in this specific context. That might mean these variables genuinely have little impact, or that the sample just isn't large enough to detect more subtle effects.

Still, the model overall shows a decent level of explanatory power. The R^2 is 0.357, meaning it explains about 36% of the variation in cybersecurity investment. The adjusted R^2 is 0.135, which adjusts for the number of predictors but still points to a usable model.

Lastly, the constant in the model is statistically significant ($\beta = 6.169$, $p < 0.05$), with a relatively large standard error (2.663). This suggests that even when all explanatory variables are set to zero, the baseline level of investment remains substantial.

Input: The first key finding is that both PU and PEoU have a positive and statistically significant effect on cybersecurity investment when tested separately in simple OLS models without control variables. PU shows a strong positive effect ($\beta = 0.377$, $p < 0.001$), and the same holds for PEoU ($\beta = 0.411$, $p < 0.001$). These results suggest that respondents who see cybersecurity measures as useful and easy to use are more likely to invest in them.

The second finding relates to the combined model that includes both PU and PEoU at the same time. While the coefficients remain positive, their individual significance disappears. This is likely due to multicollinearity: PU and PEoU are conceptually and empirically related ($r = 0.55$), which causes overlap in what they explain. Still, the model that includes both variables shows a higher

explained variance ($R^2 = 0.274$), which suggests that together they provide a more complete picture. So, while their individual effects become less clear, their combined presence in the model gives better insight into what drives investment decisions.

The third finding comes from the bootstrap analysis, which was used to test the robustness of the effects of PU and PEoU on investment. Both variables still show positive average coefficients (PU = 0.272, PEoU = 0.293), but their confidence intervals include zero, meaning the effects aren't statistically significant. This is probably due to the small sample size (n = 40) and the shared explanatory power between PU and PEoU, which makes it harder to isolate their separate impact.

The fourth finding involves the multivariate regression with control variables. In this model, neither PU nor PEoU individually shows a significant effect. However, when they are combined into a single composite variable representing cybersecurity awareness (as the average of PU and PEoU), the effect does become significant and positive ($\beta = 0.509$, $p < 0.05$), with a higher explained variance ($R^2 = 0.327$). This suggests that it's not just how useful or easy a measure is perceived to be on its own, but rather the overall awareness that drives firms to invest.

The fifth and final finding is based on the interaction model, which looks at whether there's a reinforcing effect when PU and PEoU are combined. The interaction term has a positive coefficient ($\beta = 0.143$), but it's not statistically significant. This means there's no solid evidence that ease of use strengthens the perceived usefulness of cybersecurity measures—at least not in this sample. Again, the small sample size and resulting high standard errors likely play a role in this lack of significance.

Input: The findings of this study offer several important theoretical contributions. First, this research adds to the existing literature on cybersecurity awareness. While earlier studies have pointed out a gap between awareness of cyber threats and the actual implementation of protective measures in SMEs, there's still relatively little quantitative research on how awareness influences investment behaviour (Chidukwani, Zander, & Koutsakis, 2022). Chidukwani et al. emphasize that quantitative studies on cybersecurity in SMEs are still underrepresented, and they specifically call for stronger quantitative approaches that focus on overlooked aspects—such as the practical implementation of security tools, which in this study is captured by the PEoU variable. By exploring this link in real-world SME settings, this thesis helps fill that gap. The results show that cybersecurity awareness—measured through PU and PEoU—is positively linked to how much

firms invest in security, supporting the idea that awareness does in fact shape strategic decision-making.

Second, this study addresses the lack of research on cybersecurity investment within the Dutch SME context. Most existing research focuses on large companies or international comparisons, but this study specifically targets SME retailers in the Netherlands—a group that's digitally vulnerable yet often falls outside the reach of regulations like the NIS2 directive. This makes the findings especially relevant, offering fresh insight into how firms that aren't strictly regulated approach cyber threats, and what role awareness plays in that process. This supports earlier calls by Furnell & Clarke (2012) for more context-specific research in the SME sector. The relevance of this study is further backed by recent findings from ABN AMRO (2025), which reported that one in five Dutch businesses suffered a cyber-attack in 2024, and that many SMEs are still unfamiliar with NIS2 rules (Krauwer, 2025). While the ABN AMRO study highlights the issue at the national level, this thesis adds micro-level insight into the behavioural dynamics driving cybersecurity investment in SME retailers. In doing so, it extends the literature by showing that cybersecurity awareness—measured through PU and PEoU,is positively linked to a company's willingness to invest, especially in unregulated sectors like retail.

Input: This study has several limitations that offer useful directions for future research. The first limitation is the sample size and its representativeness. The analysis is based on just 40 respondents who met the selection criteria, which limits the statistical power of the results. Because of this, many effects—while theoretically meaningful and pointing in the expected direction—do not reach statistical significance. This makes it harder to draw firm conclusions about causal relationships and reduces the extent to which the findings can be generalized to the wider SME population. In other words, external validity is limited.

The second limitation has to do with how some survey questions were worded. A few items used compound phrases or ambiguous language—for example, words like "and" or "sometimes", which can lead to differences in interpretation and introduce noise into the data. These kinds of formulations make it harder to interpret responses consistently and may affect the internal reliability of the scales used. Future research could benefit from more thorough pre-testing of the survey and clearer question design to reduce measurement error.

A third limitation is the inability to apply bootstrapping to all variables, especially the control variables. Because of the small sample size and the categorical nature of some controls, it wasn't

possible to run bootstrap analyses on the full regression models. This means the robustness of certain findings, particularly those from models with many control variables, couldn't be fully confirmed. A larger sample in future studies could solve this problem and allow for more comprehensive robustness checks.

Lastly, the cross-sectional design of this study is a methodological constraint. Since all data were collected at a single point in time, we can't track how awareness or investment intentions change over time. Nor can we make strong claims about causality. A longitudinal approach would help map how cybersecurity awareness and investment behaviour evolve, and also evaluate the long-term impact of policy interventions or awareness campaigns.

Input: This study explored how cybersecurity awareness influences the willingness of Dutch SME retailers to invest in cybersecurity measures. The relationship between awareness and investment behaviour was examined using survey data from 40 valid respondents, based on the Technology Acceptance Model (TAM).

The findings show that cybersecurity awareness—measured through perceived usefulness (PU) and perceived ease of use (PEoU)—is positively linked to investment levels. In simple regression models, both PU and PEoU are individually significant. However, their significance drops in multivariate models. When PU and PEoU are combined into a single awareness variable, this composite measure does significantly predict investment behaviour. This suggests that SME retailers are more likely to invest when they believe cybersecurity is both useful and easy to implement.

Despite some methodological limitations, this study provides valuable insights for both academic research and practical application. The results highlight the importance of awareness-raising strategies that go beyond just pointing out risks—they should also make clear how cybersecurity measures work and why they're doable for small businesses.

The central research question was:

Does the level of cybersecurity awareness affect investment in cybersecurity measures within small and medium-sized enterprises in the retail sector in the Netherlands?

Based on the results, the answer is yes: higher awareness appears to lead to higher investment levels. Awareness plays a crucial role in prompting action, even in settings where there's no legal obligation to invest. Hypothesis 1 (H1) is supported by this study, though some caution is needed

due to the small sample size, the lack of significance for PU and PEoU in multivariate models, and limited robustness checks.

Overall, the study reinforces the value of accessible and practical awareness campaigns tailored to SMEs as a key tool for strengthening digital resilience. The main takeaway is that awareness isn't the goal itself—it’s a necessary condition for building digital resilience, especially in sectors that aren't covered by legal cybersecurity mandates.