Understanding factors influencing SME's decision makers when implementing cybersecurity measures: a protection motivation perspective.

A quantitative study on the relationship between SME-decision makers' perceived protection-motivation and the implementation of basic cybersecurity measures.

Julius Offers
S2681307

Master Thesis Crisis and Security Management
Faculty of Governance and Global Affairs
Leiden University
June 2020

Supervisor: Dr. Tommy van Steen
2nd reader: Dr. Els de Busser

Table of Contents

Acknowledgements

This master thesis represents the conclusion of my academic life. A period which led me to three universities and through numerous courses over the last years. My studies introduced me to many inspirational professors, fellow students, and friends. I will always remember the good memories of my time in Tilburg, Stellenbosch and the Hague.

The process of this research started about nine months ago with a course on behavioral change approaches to cybersecurity by my thesis supervisor, Dr. Tommy van Steen. The relevancy and topicality of the subject provided the first ideas on a research related to this topic. Through this thesis I have gotten to research different interesting and relevant topics related to cybersecurity. I have gained valuable knowledge on how organizations manage cyberthreats, why such threats are too often neglected, and how to assist in coping with these threats.

The process of this thesis was, however, by no means a process I could have done by myself. I want to thank all respondents for participation. Furthermore, I want to thank Dr. van Steen for supervising me and providing support and advice during this process. Finally, I want to thank my family and friends for their help and support. Especially my parents and Eva, for their support and love through the years.

Always and forever,

Julius

List of abbreviations

CBS = Centraal Bureau voor Statistiek

DTC = Digital Trust Center

ENISA = European Union Network and Information Security Agency

E.U. = European Union

MKB = Midden en Kleinbedrijf

NATO = North Atlantic Treaty Organization

NCSA = Nationale Cybersecurity Agenda

NCSC = Nationaal Cyber Security Centrum

NCTV= Nationaal Coördinator Terrorisme en Veiligheid

ICT = Information and Communication Technology

PMT = Protection Motivation Theory

SME = Small and medium sized enterprises

ZZP = Zelfstandige Zonder Personeel

Abstract

As organizational structures are increasingly dependent on computer systems and information technology, the vulnerabilities of these systems become more and more significant to the continuity of modern organizations. The high-speed embracement of the advantages of computers must come with an equally high-speed embracement of securing these systems. Within the Dutch small and medium-sized enterprises (SME) sector, the implementation of basic security measures is widely lacking. In order to understand how current and future interventions regarding cyber resilience are interpreted within this sector, it is important to conduct theoretically based research that provides a foundation to investigate the issue. This study examines the relationship between protection-motivation factors and the implementation of cybersecurity measures within the Dutch SME sector, examined from a decision maker's perspective. By testing protection motivation factors derived from the protection motivation theory (PMT), this quantitative study displays what factors influence a SME-decision-maker when deciding to implement cybersecurity measures. Overall, a significant relationship between protection motivation factors and the implementation of cybersecurity measures is found. Higher perceived severity, perceived response-efficacy and perceived self-efficacy were associated with a greater implementation of cybersecurity measures, while higher perceived response-costs was associated with lower implementations of cybersecurity measures. No significant relationship is found between perceived vulnerability and the implementation of cybersecurity measures. This study provides a basis in understanding the different factors that influence a decision maker's behavior when implementing cybersecurity measures. The results contribute to increasing the potential impact of current and future interventions regarding cyber resilience in the SME sector.

1 Introduction

1.1 Introduction into topic

The ever-evolving issue of cyberthreats is one in which we currently face more threats than ever, each new threat being more potent and better at its job than the last (NATO, 2019). The increasing importance of information systems around the globe (Ifinedo, 2012; Tarter, 2017) and the rapid adoption and use of IT systems, social media, mobile computing, big data, cloud computing, and the Internet of Things (IoT) on a global scale causes individuals and organizations to become increasingly vulnerable to cyber-attacks (Fischer, 2014; NCSA, 2018; Notté & Slot, 2019). For organizations, the consequences of cyber-attacks vary from causing minor obstacles in day-to-day activities to producing long-term problems such as severe reputational damage, operational disruptions and the loss of proprietary knowledge (Sangani & Vijayakumar, 2012). Different studies even linked cyber breaches to businesses' downfall (Choo, 2011; Sangani & Vijayakumar, 2012). Besides affecting targeted businesses, cybersecurity breaches often affect businesses' owners, surrounding communities, partners and customers (Paulsen, 2016). Over the last few years, the number of company-related security breaches increased dramatically (Accenture, 2019; Paulsen, 2017). Currently, half of all Dutch companies has had to deal with forms of cyber-crime (Centraal Beheer, 2018), making cybercrime the leading crime against organizations (NATO, 2019).

For organizations to safeguard critical assets against cybercrimes, and to reduce the chances of being unable to functionally operate, the implementation of security tools and measures is crucial (Crossler, 2010; Ifinedo, 2012). However, over the last decade, a 'gap' in cybersecurity implementation originated between large organizations and small and medium-sized organizations (SMEs) (Hiscox, 2019; Tawileh et al., 2007). The definition of an SME, as referred to within the European Union (E.U.), is a firm with fewer than 250 employees (European Commission, 2019).Whereas larger organizations and companies often have in-house security operation centers, most small organizations are barely aware of digital risks (NCSA, 2018). Currently, only minimal cybersecurity measures are widely adopted within the SME sector, and the investments and implementations of adequate cybersecurity policies in place are regularly not sufficient (Hiscox, 2019; Osborn, 2015). For SMEs, even the most basic security measures are often lacking (NCSA, 2018). Consequently, SMEs become a weaker target for cyber criminals. This produced a growing trend of cyber attacks specifically aimed

at SMEs (Centraal Beheer, 2018; MKB, 2017; Paulsen, 2016). Currently, 43% of all organizational breach-victims are SMEs (Verizon, 2019). Research led by dr. Leukfeldt showed that one in every five SME-entrepreneurs has been a victim of cybercrime (MKB, 2017). Both the number of incidents and the volume of damage done per incident are increasing (Hiscox, 2019). As the Dutch SME sector comprises about 99% of the total number of Dutch companies and generates great social and economic value (CBS, 2019a), generating more cyber resilience is crucial.

1.2 Relevance and research objectives

Cybersecurity within the Dutch SME sector is a recognized problem that nationally coordinated initiatives such as the Digital Trust Center (DTC) (Rijksoverheid, 2018) and different trade unions (MKB, 2020) are actively concerned with. By providing practical information, advice, and offering guidelines on safe digital entrepreneurship these institutions strive to create a growing awareness within the sector. Unfortunately, these guidelines do not nearly reach all SMEs, especially not the smallest ones (Gafni & Pavel, 2019). The Dutch national cybersecurity agenda (NSCA), argues that cybersecurity is directly linked to the country's national security, and states that gaining a cyber-secure private sector is the cornerstone of achieving a cyber-secure country (NSCA, 2018). SME's are large in number, often do not have the controls in place to prevent successful attacks, and are often unprepared to manage their cybersecurity capabilities (Shojaifar et al,. 2018). Herefore, the need to build more capacity, create more knowledge, and offer perspective is urgent (NCSA, 2018).

Currently, little is known regarding what motivates SME's decision makers when deciding to implement cybersecurity measures. Multiple studies that have researched the mismatch between SME's top-management and the implementation of adequate cybersecurity measures, related the lacking implementation of security measures to a lack of awareness (Lopez-Nicolas & Soto-Acosta, 2010; Mulligan & Schneider, 2011), a lack of financial investments (Gafni & Pavel, 2019; Kajtazi & Zec, 2015), a lack of understanding (Shojaifar, 2018) or a lack of ability (Gafni & Pavel, 2019). These potential mechanisms currently are not sufficiently understood to draw firm conclusions. It is therefore important to further investigate what factors drive SME's decision makers when implementing cybersecurity measures. The lack of research in this area represents a knowledge gap, this study aims to provide an initial basis for further research of these factors.

This research aims to explore the mismatch between the implementation of cybersecurity measures and SME's decision makers. Hence, this study will generate more knowledge on what factors effect decision-makers when deciding (not) to implement cybersecurity measures. Decision-makers' protection motivation will be examined using concepts derived from Protection Motivation Theory (PMT) (Rogers, 1975). PMT, a well-supported theory in explaining protection motivation behavior, shows great promise in the cybersecurity field (Williams & Joinson, 2020). By using this comprehensive theory, this study tends to add to the current body of knowledge.

This research examines decision maker's behavior regarding the implementation of a basic level (DTC, 2020) of cybersecurity measures by analyzing whether there is a relationship between PMT-concepts and the cybersecurity 'level' of Dutch SMEs. Concepts from both a threat appraisal; assessing the perceptions of how threatened a SME decision-maker feels by cyber threats, and a coping appraisal; assessing how decision-makers perceive their ability to successfully manage cyber threats, will be used to examine the protection motivation of SME's decision-makers. In order to develop and validate the influence of the different concepts derived from both appraisals in relation to cyber-secure behavior, a number of hypotheses are formulated. These hypotheses follow a review of existing research regarding PMT and its adaption to security behaviors (Dang-Pham & Pittayachawan 2015; Herath & Rao, 2009b; Ifinedo, 2012; Williams & Joinson, 2020; Woon et al. 2005) and will be used to answer the main research question:

Are protection motivation factors related to the implementation of a basic level of cybersecurity measures within the Dutch SME-sector?

This exploratory study uses a quantitative design to test its hypotheses and answer the stated research question. Building on existing knowledge, this study creates a greater understanding of the relationship between decision-makers' protection motivation factors and the implementation of cybersecurity measures within the Dutch SME sector. Moreover, this study generates more insight into the general condition of both threat- and coping-appraisal-related factors regarding cyber risks within the SME sector. More knowledge regarding this relationship potentially provides key insights contributing to the effectiveness of future cybersecurity awareness policies aimed at SMEs. This study hence provides a more comprehensive understanding of the influence of protection motivation factors on the

implementation of cybersecurity measures within the SME sector. More practically, it contributes to the development of campaigns and training methods aimed at increasing the cybersecurity awareness of SMEs decision-makers and hence contribute to the current societal problem of overcoming SMEs backlog in cybersecurity. More knowledge on what drives decision-makers when deciding to (not) implement security measures could be of value to multiple organizations and national institutions. This study's results support in effectively informing SMEs decision-makers regarding the potential dangers and solutions that cybertechnology brings. Gaining more knowledge in this area will potentially contribute to the cyber resilience of the private sector and consequently national cyber security (NCSA, 2018).

1.3 Structure of thesis

This introduction is followed by a section containing a theoretical framework. In this section different concepts, topics, and the positioning of this research in the current body of knowledge will be clarified. The theoretical framework follows the rise of cybersecurity in current society and specifically indicates the relationship between cybersecurity and the SME-sector. Furthermore, PMT will be thoroughly elucidated and a theoretical clarification will be provided on each of the stated hypotheses. The theoretical framework section is followed by a section in which the methodology of this research is explained. This section contains clarifications on the procedures used in order to get a valid answer to the research question. This section contains a validation of the used survey, and further explains the process used in analyzing the collected data. Then, a section including this study's results follows, in which a complete, objective, and systematic reporting of the study's results is included. Finally, this research concludes with a discussion section. This section will contain a segment of this study's limitations and will furthermore include a conclusion and a discussion of how the findings relate to current research and future research.

2 Theoretical Framework

2.1 Cybersecurity as an (inter)national issue and a private business responsibility

This section provides clarity on the positioning of this research in the current body of knowledge. It will start with a wider portrayal of cybersecurity issues in (inter)national context, followed by a focus on the implications cybersecurity has on the Dutch SME sector. Thus, this section will provide the context necessary to understand the perception SME's decision makers have regarding cybersecurity issues.

The conceptualization of cybersecurity

Cyberspace has shown to be the fastest evolving technology in recent history, an area in which new and emerging properties and applications increasingly complicate the evolving threat environment (Fischer, 2014). An often-used term in literature aimed to elucidate the act of securing these online systems is 'information security', this term refers to the protection of information from possible harm incurred by various types of threats (Von Solms & Van Niekerk, 2013). Over the years the internet and digital systems acquired an increasingly interwoven character in our daily life. Von Solms and Van Niekerk (2013) stressed that the rising interconnectedness of the internet through, among other things, digital media and home automation inevitably led to an increase in new threats. These threats, no longer solely forming a danger to the security of information, expanded to forming a danger to resources, assets, and humans, with effects ranging from individuals up to a national or even international level. The use of the term 'information security' did no longer suffice, as it no longer met the standards of securing all that is threatened (Von Solms & Van Niekerk, 2013). This situation led to the adoption of the term 'cybersecurity', a term in which not the protection of solely cyberspace as an asset, but the protection of all that functions within cyberspace and any asset that can be reached via cyberspace is included (Von Solms & Van Niekerk, 2013). This research intends to use the more inclusive term cybersecurity, however, in instances were the original source makes use of the concept information security in explaining the protection of cyberspace, this term is used.

Cybersecurity is a broad and somewhat fuzzy concept that is often conflated with other concepts such as privacy, intelligence sharing, information sharing, and surveillance (Fischer, 2014). Originated in the early 1990s, information security is first used to underline insecurities related to networked computers. Major global events, such as the Twin Towers attacks on

September 11th, 2001 spurred the attention given to information technology in a global security manner (Hansen & Nissenbaum, 2009). Cybersecurity, having implications for national security, the economy, human rights, civil liberties, and international frameworks, emerged as one of the most challenging aspects of our age for policymakers and scholars of international relations (Carr, 2016). Built on the Copenhagen School of thought, Hansen and Nissenbaum (2009) described 'cybersecurity' as 'computer security' plus 'securitization'. The success of the securitization of cybersecurity in nation-state security departments is indicated by the creation of a NATO-backed cyber defense center, and European Commission led organizations such as the European Union Agency for Network and Information Security (ENISA) (Hansen & Nissenbaum, 2009). Cybersecurity is now a globally recognized threat that governments are increasingly occupied with. Opposing the ever-evolving threats the internet brings, both ENISA and NATO currently acknowledge the extent of the matter and recently asked for a more cooperative approach in dealing with the issue (EC, 2019; NATO, 2019).

From national governance to a private business responsibility

The Netherlands has to deal with different forms of digital threats on a daily basis. Characterized as fast, hyperconnected, and extremely complex, failure or disturbance of the digital domain potentially has consequences for all layers of Dutch society. Herefore, digital safety is an urgent issue that requires immediate attention and asks from everyone to be alert and adopt a hands-on mentality (NCTV, 2020). In developing national cybersecurity strategies, the government defined the security of critical infrastructure as a key factor in achieving national cybersecurity. The Dutch national cybersecurity agenda concluded that cybersecurity is solely achievable when collaborating with the private sector. Consequently, public-private partnerships are seen as the core of the Dutch cybersecurity approach (NCSA, 2018). Mainly the impact the internet potentially has on national economies, makes the business-sector a key focus (Carr, 2016). Following European laws, owners and operators of digital infrastructure are, by Dutch law, required to take appropriate technical and organizational measures to manage cyber threats and prevent incidents (NCTV 2020; Rijksoverheid, 2018). However, the government remains largely dependent on private companies' personal initiatives to safeguard the national security. More than 80 percent of the complete critical infrastructure in the Netherlands is owned by private companies. The government is typically not able to regulate the cybersecurity measures within these companies (NCTV, 2020).

In order to assist the private businesses sector in increasing cyber resilience, governments tend to use a cooperative approach. Cooperation between the government and private companies, aimed at increasing cyber resilience, is often referred to as 'public-private partnership'. The term 'partnership' points to the way in which private organizations and businesses are part of solving the same issue (Hansen & Nissenbaum, 2009). Examples of public-private partnership are the Digital Trust Center (DTC), the National Cyber Security Center (NCSC), and the Computer Security Incident Response Team for Digital Service Providers (CSIRT-DSP). The DTC, established in 2018, supports Dutch organizations that are considered as not vital in creating cyber resilience. The institution targets all businesses in the Netherlands that are not appointed critical infrastructure, but mainly focuses on SMEs (DTC, 2020). The DTC supports businesses by sharing accurate, up-to-date, and reliable advice and furthermore grants subsidies via cyber resilience networks. These networks are formed by groups of organizations and are meant to increase the cybersecurity within a particular region, sector, or supply chain (DTC, 2020). The NCSC fulfills this purpose for the Dutch private sector marked as vital. The CSIRT-DSP is charged with receiving incidents from digital service providers, with the aim of reducing the economic and social damage of major incidents. The CSIRT-DSP furthermore warns other digital service providers of ongoing incidents and shares the current intelligence with its constituency (CSIRT-DSP, 2019). All different projects and pilots and every cooperation essentially aims to increase awareness and resilience for businesses (Grapperhaus, 2019).

In these strategies, the political center, while offering assistance and guidance, considers the private sector as responsible for major parts of national cybersecurity (Hansen & Nissenbaum, 2009). Cybersecurity in this sense implies that both public-private responsibility and governmental authority share the same goal. The Dutch government 'expects' the private sector to take its responsibility and contribute to the issue (NCSA, 2018). From a governance perspective, considering cybersecurity as a common good, the business sector is an essential factor in attaining the goal of a cyber-secure society. This relationship, although described as the 'cornerstone' of national cybersecurity, is a relationship which lacks explicitly defined parameters and consequently causes fundamental disjuncture between the expectations of all parties involved (Carr, 2016). The language chosen by governments in forming such relationships is deliberately picked to avoid suggestions of hierarchy but rather tries to imply a shared purpose and a shared interest (Carr, 2016). Carr (2016) suggests that the use of this 'shared-purpose-language' belies the alignment of perceptions on a common purpose, and the

threats faced with. The partnerships often remain at a rhetoric level and do not correspond with the interest of most private entities (Bossong & Wagner, 2016). The private sector, viewing cybersecurity challenges predominantly as financial or reputational risks, is often not too concerned with national cybersecurity as a common public good and will never invest in cybersecurity beyond its cost/benefit analysis (Carr, 2016). Dutch SME's decision makers are responsible for the cybersecurity within their organization; it is however at the interest of the government that these organizations maintain, or reach, an adequate level of cybersecurity.

The relationship between private organizations and the government indicates the complexity that lies in national cybersecurity issues and displays the responsibility private organizations are handed regarding the issue. Although intentions from organizational measures such as the DTC and initiatives at local municipalities are helpful and relatively successful in increasing awareness within the SME sector (Grapperhaus, 2019), cyber threats still remain each and every SME decision maker's responsibility. This research will continue to focus on the management of the threats private organizations primarily have to cope with, emphasizing the responsibilities SME's have regarding the cybersecurity of their business.

The management of SME's cyberthreats

From a private-organization perspective the responsibility regarding cyber threats is the responsibility to secure against any danger to the organization's continuity and accepting this responsibility as part of a cost/benefit framework (Carr, 2016; Posthumus & von Solms, 2004). Cybersecurity in this sense is seen as a management responsibility, a business priority that demands the attention of the board and the executive management within any organization. The management of information security is a responsibility formulated through the implementation of procedures to counteract risks (Posthumus & von Solms, 2004). Information security management is concerned with how this responsibility is translated within the organization. In terms of SMEs, depending on size, this responsibility mostly comes down to the highest decision-maker within the organization or, if present, an IT department/chief IT (Posthumus & von Solms, 2004).

For private-sector businesses, cybersecurity should be seen as a method to reach the organization's main goal: making profit. When analyzing cybersecurity as a way to reach this goal it is the organization's top-level that is responsible to establish the organization's security

systems and its overall objectives and priorities in order to support the mission of the organization (Guttman & Roback, 1995). Securitizing information is a concern which everyone using any form of IT services should bear in mind (Siponen, 2001).

Siponen (2000) refers to information security awareness as a state in which users are aware of their security mission. In academic literature, cybersecure behavior is often related to the awareness of employees with regards to cybersecurity. In these articles security awareness is often used to indicate the level of commitment an employee shows with regards to the cybersecurity policy. For example, in studies indicating that a higher level of awareness has a significant effect on end-user's ability to distinguish fraudulent emails and websites (Alwanain, 2019). Individuals in these studies are seen as potential abusers of cyber-systems, and researchers examine ways to discourage the intentions that potentially lead to breaches of computing systems (Lee & Lee, 2002). This research will concentrate on an individual's potential as a protector (Lee & Lee, 2002), by focusing on the cybersecurity protection motivation within higher organizational levels. Through this lens cyber-secure behavior is the top management, the director of an SME, a final decision-makers, or an entrepreneur, making the decision to adopt adequate cybersecurity measures. It is the top management's responsibility to ensure that the so-called CIA triad: confidentiality, integrity, and availability of business-related information is maintained (Fischer, 2014). The security policy functions as a mean to highlight the importance of security goals and objectives (Posthumus & von Solms, 2004).

2.2 Cyber risks

In order to understand the necessity of implementing cybersecurity measures, it is essential to first review what risks cyber threats impose to Dutch SMEs. The management of these risks is fundamental to effective cybersecurity (Fischer, 2014).

A risk is often described as the possibility of loss, generally explained consisting of two compontents: the probability and the severity of negative outcomes (Van der Pligt, 1996). A cyber risk is the overall harm that may occur after a security breach. Potentially, this can be any event having a negative effect on the availability, integrity, confidentiality, and authenticity of network- and information systems (NCTV,2020). The impact of cybercrime can result in the loss or damage of financial, proprietary, or personnel information from which the attacker

can benefit (Fischer, 2014). These effects may often have short-term consequences in cases of small errors, a short service denial, or a brief disclosure, but can be extremely impactful when organizations face their long-term consequences (Guttman & Roback, 1995; Choo, 2011; Sangani & Vijayakumar, 2012).

Concepts of businesses' cyber risks

Early forms of Malicious Software (malware) were first found in the 1980s, during this period of time viruses were primarily passed by exchanging infected disks. The growth of the World Wide Web and browser software in the early to mid-1990s fueled increasingly destructive threats such as malware and other forms of computer crime (Yost, 2007). As the internet evolved from an experimental network that solely allowed resource sharing, into a global platform for personal communications and commerce that expanded into business context across the globe, the importance and complexity of its security increased drastically (DeNardis, 2007).

The evaluation of cyber-risks for a private business is mainly formed by four concepts: threats, vulnerabilities, safeguards and assets (Guttman & Roback, 1995). Threats are entities or events that potentially harm the system. In order to determine the likelihood of occurrence and potential harm, these entities have to be identified and analyzed (Guttman & Roback, 1995). In a more specified sense, the people that actually perform cyberattacks can be divided into one or more of five categories: terrorists, engaging in cyberattacks as a form of non-state or state-sponsored warfare; hacktivists, performing cyberattacks for nonmonetary reasons; nation-state warriors, undertaking cyberattacks in support of a country's strategic objectives; spies, intending to steal classified information used by private entities or governments' and criminals; performing crimes such as theft or extortion in order to gain monetary benefits (Fischer, 2014). In 2019, 71% of all breaches worldwide were financially motivated (Verizon, 2019). Hacking, ransomware, phishing messages, and viruses are different modern examples of cyberattacks aimed at organizations, such attacks are primarily used by criminals (Tarter, 2017).

Organizations' vulnerabilities are the weaknesses that could be exploited by threats. As ICT systems are often very complex, and attackers are constantly probing for weaknesses, cybersecurity is often seen as an arms race between attack and defence (Fischer, 2014). Vulnerabilities allow for systems to be harmed and are often analysed in terms of missing

safeguards (Guttman & Roback, 1995). Not implementing a firewall, for example, is a vulnerability to a company's cybersecurity. Humans, the defenders of information systems, are often seen as vulnerabilities, as they potentially bring limitations such as having an incomplete picture of the situation and regular human biases (Dykstra, 2015). Hence, the decision maker could be a potential vulnerability to an SME's cybersecurity. Vulnerabilities are present in many different aspects within any running company. Weaknesses can differ from business to business. Suppliers and technology providers, supporting organizations, and employees, all have an effect on the number and extent of weaknesses a company is faced with (Guttman & Roback, 1995). Additionally, modern and rising functions such as maintaining a website, performing e-commerce and using cloud computing are all vulnerabilities that need careful treatment in order to cope with possible cyber-attacks (Gafni & Pavel, 2019).

Safeguards are actions, devices, techniques, procedures or other measures that reduce the vulnerabilities in a system (Guttman & Roback, 1995). The goal of these safeguards is to defend a network, data, or its users. In order to do so, defenders must be knowledgeable of the state of security they are in. Some threats, such as computer viruses and infections, ask for caution from every individual within the organization, as one individual behaving irresponsibly potentially endangers the safety of the whole. Such threats support the fact that the individual not solely functions as a responsible partner in fighting insecurity, but also forms a potential liability or threat (Hansen & Nissenbaum, 2009). As presented, in cybersecurity, employees are often seen as the weakest link in an organization's security chain (Pfleeger et al., 2014).

Assets include all of value that might be impacted in the short- or long-term as a consequence of a cyber threats (Guttman & Roback, 1995). To grasp the size of cyber threats it is required to comprehend the networked character of computer systems, in which the danger mostly lies in the potential consequences for objects beyond the networks itself (Hansen & Nissenbaum, 2009). Not solely assets online are potentially in danger, but all assets that are linked to computer systems and networks are. Mulligan & Schneider (2011) state that absolute cybersecurity is not affordable, but also, for most systems, not necessary. When regulating the cybersecurity of an organization it is important to find the balance between the implementation of measures and the risks taken by not doing so. For private businesses, cybersecurity potentially posing a risk to assets such as finance and reputations will always be seen in the light of a cost/benefit analysis (Carr, 2016).

2.3 Cyber security measures

Computer security, an aspect of digital computing for decades, grew to a fundamental concern for governments, corporations, and other organizations (Yost, 2007). Cyberspace however is a constantly changing phenomenon, therefore often highly complex and difficult to secure (Dykstra, 2015). Information security management is the continuous process of carrying out the necessary activities that facilitate the preservation of an organization's business (Posthumus & von Solms, 2004). The increasingly ubiquitous issue of computer and network security requires a multifaceted approach (Yost, 2007). The effective management of cybersecurity requires a combination of both technical and procedural controls (Kruger & Kearney, 2006). It is the purpose of computer security management to protect an organization's valuable resources by selecting the appropriate safeguards (Guttman & Roback, 1995). Examples of such measures are: installing firewalls, updating, using anti-virus software, backing up their systems, maintaining and restricting access controls, and using comprehensive monitoring systems (Ryan, 2004, Lee & Larsen, 2009). Cybersecurity functions as an instrument to protect privacy and prevent unauthorized surveillance and is meant to protect an organization's ICT systems' confidentiality, integrity, and availability (Fischer, 2014). The optimal level of risk reduction varies among sectors and organizations but usually involves removing the threat source, addressing potential vulnerabilities, and lessening impacts (Fischer, 2014). It may sometimes be difficult for an organization to approach the risks that cyber threats bring as cybersecurity approaches, just as cyber threat approaches, evolve as technology changes over time (Asllani et al., 2013). A critical first step in the understanding of cybersecurity is acknowledging the fact that there will always be threats, infiltration, and destruction. The way of coping with these threats is where the difference is made.

Although crafting a completely cyber-secure company is almost impossible, there are multiple measures that reduce the chances of cyber threats harming the organization. Assisting SME-owners in applying the necessary 'basic' cybersecurity measures, the Digital Trust Center specified five basic principles of 'safe digital entrepreneurship'. These five principles; (i) make an assess of vulnerabilities, (ii) use safe settings, (iii) make sure to update, (iv) limit access, and (v) prevent viruses and malware, are meant to provide a basic layer of security, protecting organizations against the majority of cyber breaches (DTC, 2020).

Make an assessment of vulnerabilities

The first step in achieving a cybersecure organization is assessing the vulnerabilities within the organization. By doing so, a decision-maker is forced to think about what to do in case of a cyber-emergency. Assessing vulnerabilities is vital when creating an emergency-plan that comes into force in case of a cyberbreach. The assessment will display the vulnerable parts of the company by analysing availability, integrity and confidentiality (Fischer, 2014).
Assessing availability will indicate how harmful the effects are if particular systems within the organization would stop functioning. Integrity stands for the maintaining of the accuracy and completeness of data (DTC, 2020). Assessing integrity-vulnerabilities within an organization will present how damaging the effects would be if, due to a cyberbreach or attack, certain information becomes incorrect or incomplete (DTC, 2020). Assessing confidentiality, indicates how bad the results will be if information leaks or otherwise becomes available to unauthorized individuals, entities or processes. It is of great importance to get an insight into these risks in order to realize a good defence. Assessing vulnerabilities is crucial when considering what measures to implement and where to invest in (DTC, 2020).

In case of cyber-incidents, an assessment of vulnerabilities helps to focus on keeping the essentials safe and prioritizing the importance of systems. An important technical measure regarding this principle is making back-ups. A back-up is used to recover lost data. In situations of system errors, accidents, stolen or broken devices, viruses or system-damages a back-up can be of great value. The best way to store a back-up is, disconnected from a network, preferably encrypted, on a safe location (DTC, 2020).

Use safe settings

Device-suppliers often apply default-settings to their devices. SMEs using such devices on default settings are extremely vulnerable to cyber threats. These devices are, in a worst-case scenario, directly accessible from the internet. Cybercriminals use automated programs that specifically search for such weaknesses. Hence, cybercriminals are potentially able to access and alter all information stored in devices, software and networks within the company. Functions such as webcams and microphones might even be remote-controlled by criminals (DTC, 2020).

To ensure the use of safe setting, different cybersecurity measures are needed. The DTC (2020) mentions three measures to increase cybersecurity. Firstly, stressing the necessity to check and adjust default settings. Furthermore, they advise to use safe, strong, and unique passwords. Developing, using, and frequently varying the routine of complex passwords can make computer crime far more difficult (Yost, 2007). Vital systems, such as banking details and crucial company information require extra security. Using two-step-verification or a login-token are both suggested examples of such security. Finally, in order to defend the company-network from other networks, it is highly recommended to use a firewall. A firewall analyzes in- and outgoing traffic on the company's network and determines what should, and what should not be allowed access (DTC, 2020).

Make sure to update

Manufactures of devices and software constantly improve and adjust their products. Updates make sure to get these latest improvements functioning at the end-user level. A great part of these updates are improvements and patches concerned with solving discovered vulnerabilities or generally with improving security. The danger lies in cybercriminals abusing vulnerabilities in older versions of devices and software. It is therefore highly recommended to always directly install the latest security updates. This goes for all devices that are connected to the internet (DTC,2020). The practical cybersecurity-measure concerned with this principle is to always keep an eye on updates for all devices and software, if the latest update is not yet installed, directly installing updates and patches is highly recommended. If possible, it is recommended to use automatic updates. For SMEs with employees, it can be helpful to create a company-wide 'update-policy' (DTC, 2020).

Limit access

In order to limit the chances of accidents and abuse of information systems, it is important to make sure that everyone, both employees and customers, are solely allowed to strictly access the systems that fit their needs. Restricting access is meant to lock down the ability to view sensitive information, control data modification, and limit the ability to alter information. Extensive access, especially during a longer period of time, should only be allowed to those who can't go without. Open systems in which every individual is able to access all information are extremely vulnerable to cyber-criminals. Governing what people can access when and how helps to prevent this (DTC, 2020).

The basic measures regarding this principle start by defining which employee is allowed to which exact system and what parts of information. Such measures can be maintained by employees verifying their identity when logging in to particular systems. Furthermore, physical access of employees to areas in which vital systems, devices such as hard drives or USB-sticks, and documents are accessible should be limited. A more open system provides more opportunities for criminals. Finally, it is helpful to make sure that devices auto-lock after a few minutes, this prevents unauthorized access (DTC, 2020).

Prevent viruses and malware

Malware is the term for software with malicious intent. Different types of malware are deliberately spread to damage systems or devices, steal data or company-secrets, or to blackmail companies with ransomware. Malware is malicious software that disturbs systems and collects and encrypts information. Malware can enter computers, smartphones, or networks in different ways. This happens, for example, when an end-user opens an infected email or attachment, visits a malicious website or uses an 'infected' USB-stick. Once the malware has entered a system it is often able to spread to other devices and/or users. Thus, it is of great importance to prevent malware from entering in the first place (DTC, 2020).

The DTC advises different measures in securitizing against malware and viruses. First, it is important to stimulate employees to act cyber-secure. Make sure they are familiar with the dangers of phishing, malicious USB-sticks and being messy with (weak) passwords. Secondly, it is important to install antivirus programs. Such programs scan devices on malware and help prevent the spread of malware to other users and customers. Thirdly, it is necessary to be cautious with the installation of applications on online devices. When doing so, always make sure to check the sources and solely install what is essential. In order to prevent malware, avoid installing irrelevant apps, such as games, in a combination with business-related environments and never allow full access to the camera, location, contact, or payment details. Finally, it is important to make sure employees are limited in their possibilities to install software on company-devices (DTC, 2020).

2.4 SME's cybersecurity

SME's cyber threats

Historically, SMEs have primarily been active in a local environment. When the internet provided first opportunities for businesses to reach new and larger markets by accommodating opportunities to reach out to partners, customers, and employees from around the world, SMEs immediately started to take advantage of this technology (Gafni & Pavel, 2019). Computer-based tools, besides providing new business opportunities, also offer opportunities for running businesses to work more efficiently (Gafni & Pavel, 2019). Consequently, over the last two decades, organizations quickly started to adopt the advantages of computer-based tools in their daily work and business strategies (Gafni & Pavel, 2019). Cyber threats, coming in many different forms, oppose risks to any business using the internet (Guttman & Roback, 1995). The increasing dependency on information systems in which organizations, and their internal systems, are constantly connected to the internet increased the number of cyber vulnerabilities (Iloven & Virtanen, 2013).

Recently, cybersecurity attacks specifically aimed at SMEs are increasing in numbers (Bada & Nurse, 2019; Centraal Beheer, 2018; MKB, 2017;Paulsen, 2016).One in every five Dutch SMEs has currently been a victim of some sort of cybercrime (MKB, 2017) and the number of incidents is growing (Hiscox, 2019). Concurrently, Dutch SMEs are not sufficiently secured. Adequate cybersecurity policies are regularly insufficient and only the very minimal measures are widely adopted (Hiscox, 2019; Osborn, 2015; Shojaifar et al., 2018). The use and deployment of basic cybersecurity countermeasures is often lacking (Valli et al., 2014) and small businesses often pay little attention to the threats opposed by hackers, cybercriminals, and malicious insiders (Alshboul & Steff, 2018). SMEs' investments in the cybersecurity field are, compared to larger organizations, relatively low (Gafni & Pavel, 2019; Kajtazi & Zec, 2015). The lack of adequate security measures is one potential reason why the number of attacks against SMEs has grown (Bada & Nurse, 2019). As large organizations heavily invest in cybersecurity, criminals are turning their attention to smaller businesses (Alshboul & Streff, 2018). It is fundamental for SMEs to protect their customers' sensitive data and protect its intellectual property to remain competitive (Alshboul & Streff, 2018). To cope with these threats, the security of information systems is crucial (Herath & Rao, 2009a). Moreover, it is significant for the continuity of SMEs to avert these attacks by implementing adequate cybersecurity measures.

SME's lacking cybersecurity

Violations of cyber security and privacy in both personal and work environments caused academic attention on this subject to take on paramount importance (Boss et al., 2015). However, whilst different studies report of the threat cyber-issues potentially impose to businesses, very few are focused on SMEs (Valli et al., 2014; Alshboul & Streff, 2018). Academic studies that have researched the reasoning behind lacking cybersecurity measures amongst SMEs, found that SMEs often wrongfully assume they are not in danger of cyber-attacks. Not implementing cybersecurity measures then relates to the gap between the top management and information security concerns (Siponen, 2001).

A tendency of assuming not to be 'big' or 'interesting' enough to be the aim of a cyber-attack seems to prevail (Centraal Beheer, 2019; Sangani & Vijayakumar, 2012). SMEs often display a 'it won't happen to me' attitude (Scully, 2014). This is emphasized in multiple studies indicating that decision-makers within SMEs often do not see their company as a liable target for cyber-crime attacks (Gafni & Pavel, 2019; Sangani & Vijayakumar, 2012). Independent research conducted by Ipsos (Allianz, 2019) shows that more than half of all Dutch SMEs don't 'worry' about the safety of their customer- and company-data. Consequently, a lot of SMEs just turn a blind eye to cybersecurity (Sangani & Vijayakumar, 2012). A factor reinforcing this problem could be the fact that SMEs often receive information through mass communication media channels. Websites, radio, and television being SME decision-makers' primary source of instruction, often solely report about the cyber-breaches and attacks on larger organizations and government entities. Media reports publishing on cybersecurity breaches often tend to leave the smaller cases out (Gafni & Pavel, 2019). Breaches victimizing large firms and attacks on nation-states, such as respectively the ransomware-attack aimed at Maastricht University (NOS, 2019) and the well-known virus 'Stuxnet', receive national attention. Furthermore, not all information about threats and attacks is publicly available (Mulligan & Schneider, 2011). Companies that have been victimized by cyber breaches are often hesitant to display this, a given that from an organization perspective is understandable, but certainly does not contribute to an increase of the general risk perception. In this scenario SME's decision-makers simply don't know about the potential danger within their sector.

As SMEs often do not need to cope with the same complexity of information systems as large firms do, a tendency to not appoint an Information Technology (IT) department or an IT

specialist consequently grew within these companies (Lopez-Nicolas & Soto-Acosta, 2010). Therefore, the responsibility regarding the securitization of the businesses' online environment often comes down to decision-makers that do not necessarily have sufficient knowledge (Lopez-Nicolas & Soto-Acosta, 2010). The responsibility hence comes down to decision-makers that may not always be able to adequately implement a cybersecurity policy whilst dealing with the organization's daily businesses (Gafni & Pavel, 2019). Another factor potentially influencing a decision-maker's cybersecurity measure implementation behavior is found in the way decision-makers characterize and evaluate cyber risks. This is partly determined by risk perception (Slovic et al., 1982). A risk can mean different things to different people, the level of expertise on a certain subject plays a part in the judgment of a risk (Slovic et al., 1982; Van der Pligt, 1996). In the perception of risks, small probabilities are often overestimated, and large probabilities are underestimated (Van der Pligt, 1996). More 'sensational' risk situations tend to cause a too high risk perception, while more common risks tend to cause a too low risk perception (Van der Pligt, 1996). Having difficulties in understanding probabilistic processes can cause risks to be misjudged or uncertainties to be denied (Slovic et al., 1982). In analyzing a person's risk perception, it is important to not solely focus on cognitive factors. Motivational factors, such as self-efficacy, may influence the perception of risk (Van der Pligt, 1996).

2.5 Protection Motivation Theory

Responsible decision-makers need to establish adequate cybersecurity policies; however, if the importance of these practices is not understood, or the willingness to apply these policies is missing, these efforts will fail (Herath & Rao, 2009b). In a literature review study on information security and behavior studies, Lebek, Uffen, Neumann, Hohler & Breitner (2014) identified Protection Motivation Theory (PMT) as one of four major theories to explain information security behavior. Protection motivation theory is a behavioral theory that explains the effects of fear appeal on persuasion (Rogers, 1975).

The theory focuses on factors that may influence people's intentions to engage in different behaviors (Milne et al., 2002; Williams & Joinson, 2020). PMT proposes that protective behavior is motivated by both a threat and a coping appraisal. Originally, the theory states that the effectiveness of a coping appraisal, the probability of a threat to occur, and the severity of that threat, all have an effect on behavioral intentions to adopt protection motivation behavior

(Rogers, 1975). A later version of the theory added "self-efficacy" as a component (Maddux & Roger, 1983) when indicating a relation between a person's belief on whether he or she is capable of performing a particular behavior and the intentions to adopt protection motivation behavior.

Over time the theory became a leading theoretical foundation used in research to help motivate individuals to change their security-related behaviors to protect both themselves and their organizations (Boss et al., 2015).The theory shows great promise in the cybersecurity field (Williams & Joinson, 2020), specifically as a method for analyzing security awareness (Hanus & Wu, 2016). In relation to cyber-secure behavior, researchers have used and adapted different versions of existing PMT scales to different cyber security issues. Herath & Rao (2009b), for example, found that threat perception on the severity of breaches and perceptions of response efficacy are likely to affect policy attitudes regarding information security. Furthermore, an employee's intention to comply with information security policies is significantly influenced by, inter alia, self-efficacy (Bulgurcu, et al. 2010). Other studies have linked PMT scales with cybersecurity behaviors such as securing home wireless networks (Woon et al. 2005), the use of anti-spyware software (Chenoweth et al., 2009), the use of back-ups on a personal computer (Crossler, 2010), mobile users' anti-viruses software adoption (Al-Ghaith, 2016), analyzing internet users' online safety intentions (Tsai et al., 2016) and analyzing the factors that influence whether people choose to keep up to date with protective information about phishing (Williams & Joinson, 2020).

PMT's appraisals

The different components of protection motivation theory can be divided into two appraisals, both motivating protection behavior the theory consists of a threat appraisal and a coping appraisal. This section will further explain the different concepts used in both appraisals.

The coping appraisal relates to how people perceive their ability to successfully manage a threat (Woon, Tan & Low, 2005). The appraisal consists of three components; (i) response efficacy, the belief in a certain coping mechanism reducing the threat, (ii) perceived self-efficacy, the level of confidence in one's ability to implement a certain coping mechanism and (iii) response costs, the belief of how costly performing a certain coping mechanism will be (Dang-Pham & Pittayachawan 2015; Herath & Rao, 2009b ;Rogers, 1983).

The threat appraisal relates to the perceptions of threat and consists of (i) perceived severity, the degree of harm associated with the threat, and (ii) perceived vulnerability, the probability of the threat occurring. The probability is an estimation of the frequency or chance of a particular threat from happening, the severity is the potential damage of a particular threat (Guttman & Roback, 1995). Perceived severity is associated with the consequences of a cyberbreach (Ifinedo, 2011), perceived vulnerability with the assessment of the probability of a cyberthreat harming the organization (Dang-Pham & Pittayachawan 2015; Herath & Rao, 2009b; Ifinedo, 2011; Maddux & Rogers, 1983).

Different studies make use of a PMT framework in which a third component complements the threat appraisal. In these studies, rewards are the positive aspects of risky behavior. Saving time or money by not implementing cybersecurity measures, is hence seen as a negative influence on the threat appraisal. Multiple studies using PMT applied to cyber/information security behavior, however, tend to not use this variable (Chenoweth et al., 2009; Crossler, 2010; Ifinedo, 2012; Lee & Larsen, 2009; Williams & Joinson, 2020). The coping appraisal concept 'response costs', measuring the belief of how costly a particular behavior is, will to a large extent measure the same values as the concept 'rewards' will. When reviewing both concepts within the cost/benefit relation an SME decision-maker does, the cost of implementing cybersecurity measures or the rewards of not implementing cybersecurity measures will to a large extent come down to the same values. Herefore, this study will not further treat 'rewards' as a separate concept. The threat appraisal is comprised of perceived vulnerability and perceived severity (Ifinedo, 2012).

Thus, an increasing perception of a threat's severity and vulnerability is considered to increase protection motivation. Furthermore, greater consideration of an individual's ability to cope with a threat and increasing trust in the measures are considered to increase protection motivation. On the other hand, if people consider a threat to be high, but feel like they are unable to cope with that threat, a situation can emerge in which people use maladaptive coping strategies focusing on feelings of fear, such as avoidance or denial of the issue (Williams & Joinson, 2020). Meta-analysis investigating the role of these components shows that increasing vulnerability, threat severity, self-efficacy and response efficacy facilitate adaptive intentions or behaviors. Decreasing response costs and maladaptive response rewards can facilitate both the intentions to engage in future behaviors and the implementation of protective behaviors

(Floyd et al., 2000). As a well-supported theory in explaining cyber-secure behavior, PMT will serve as a suiting theory to explain an SME's decision-maker's behavior on the implementation of cybersecurity measures.

Hypotheses

This section will contain a more substantive explanation of the different PMT-factors and their expected relationship with protection motivation behavior. Following PMT's concepts, each concept, derived from either the threat or coping appraisal, will be explained. The clarification of each concept will be followed by an application to this study and hence lead to the formulation of a hypothesis.

From a SME-decision-maker's perspective, the threat appraisal is an assessment of the level of danger posed by a security event (Crossler, 2010) and can be visualized in terms of the assessment of the consequences of a potential security breach (severity) and the probability of exposure to a security threat (vulnerability) (Herath & Rao, 2009b). These statements are formulated in the following hypotheses.

Perceived severity in this study indicates the assessment of the consequences of a cyberbreach for a particular SME. In this study perceived severity is measured by assessing a decision maker's perspective on the consequences of a cyber breach within a SME. Perceived severity is expected to contribute to the likelihood of an individual deciding to implement cybersecurity measures. Following this concept, the first hypothesis is as follows:

H1: *Greater perceived severity of cyber threats has a positive effect on the implementation of cybersecurity measures*.

A decision-maker's perceived vulnerability relates to the assessment of the probability of threatening events (Ifinedo, 2012). In this study, this perception relates to a decision maker's assessment of his/her SME's falling victim to a cyber-attack. In other words, the decision maker's perception on the likeliness of a cyberbreach taking place at his/her organization. Vulnerability is perceived by an assessment of the exposure of the organization and its system when it comes to cyber threats. An individual decision-maker that assesses his/her organization

to be in great danger of cyberthreats, is more likely to implement more cybersecurity measures. The second hypothesis used to explain protection motivation behavior is as follows:

H2: *Greater perceived vulnerability of cyber threats has a positive effect on the implementation of cybersecurity measures.*

The coping appraisal is an individual's assessment of his or her ability to perform a certain behavior, and his or her confidence that this behavior will be adequate in mitigating or averting potential damage from a threatening event, at a perceived cost that is not too high (Crossler, 2010; Woon et al. 2005). From a SME's decision-maker's viewpoint, this appraisal relates to an individual's assessment on his or her ability to avert the dangers of cyber risks. The coping appraisal is composed by: the belief to what extent it is possible to implement measures in order to cope with a cyber threat (response efficacy), the belief the decision-maker is able to implement these measures (self-efficacy) and the belief about the costs of implementing these measures (response costs) (Herath & Rao, 2009b).

Response efficacy relates to the perception about the perceived benefits of the action taken by the individual (Rogers, 1983). In the context of this research, response efficacy refers to a decision maker's confidence in cybersecurity measures preventing cyber-attacks. Response efficacy relates to the confidence in security measures preventing losing financial and personal information (Ifinedo, 2012) and providing a feeling of safety when it comes to cybersecurity. More confidence in the effectiveness of these security measures will increase the likeliness of a decision-maker implementing them. Following these expected effects, the third hypothesis is formulated as follows:

H3: *Greater perceived response efficacy of cyber measures has a positive effect on the implementation of cybersecurity measures.*

Increasing self-efficacy emphasizes growth in an individual's ability or judgement regarding his or her capabilities to perform the recommended behavior (Woon et al. 2005). For this research this factor emphasizes the sorts of skills and measures needed to protect information (Van der Pligt, 1996; Woon et al. 2005). The confidence a SME's decision-maker has in having the necessary expertise to implement adequate measures to protect the digital environment of its organization (Ifinedo, 2012). If an individual's self-efficacy regarding the ability to

implement these measures grows, the implementation of these cybersecurity measures will increase. This leads to the fourth hypothesis:

H4: *Greater perceived self-efficacy with regards to cyber measures has a positive effect on the implementation of cybersecurity measures.*

Response costs stresses the perceived opportunity costs in terms of monetary, time, and effort that comes with adopting the recommended behavior (Ifinedo, 2012). In this instance the costs of implementing cybersecurity measures. In an organizational setting, such decisions are often made after making a cost-benefit analysis. The thoughts of having to spend a great number of overhead costs or time when implementing adequate cybersecurity measures decreases the likelihood of an individual implementing these measures (Ifinedo, 2012). Increasing response costs will hence lead to a decrease in the implementation of cybersecurity measures. Consequently, the final hypothesis is formulated as follows:

H5: *Greater perceived response costs has a negative effect on the implementation of cybersecurity measures.*

3 Methodology

3.1 Research Design

This empirical research analyzed the relationship between protection motivation factors and the implementation of a 'basic' cybersecurity level (DTC, 2020). To be able to draw a general conclusion on the relationship between Dutch SME's decision-makers' protection motivation and the implementation of cybersecurity measures this study used a deductive approach. A field study using survey methodology is used to examine all concepts related to both threat and coping appraisals of decision-makers within the Dutch SME sector. This quantitative study intended to test whether a relationship between the level of cybersecurity measures implemented, and protection motivation factors as perceived by a SME decision-maker are found. By analyzing a large population on different motivational factors, a comparison is made between different motivational factors and their influence on SME's decision-makers' protection motivation. The survey is used to collect information from a sample of individuals through their responses to, primarily Likert-scaled, questions. The survey is deployed in a quantitative manner by using close-ended questions only. To test the stated hypotheses this study used statistical analysis. In the following section, the details regarding the instrument development and survey administration process will be further discussed.

3.2 Respondents

This study aimed to analyze the protection motivation of SMEs' decision-makers responsible for cybersecurity within their organization. Following the European Commission's (2019) guidelines on SMEs, within this study, any company with up to 250 employees is regarded as a SME. No distinction is made in addressing SME decision-makers operating in a particular sector or region. For the purpose of this study, a distinction between a 'regular' employee and a responsible decision-maker was necessary. The survey aimed to specifically reach the person responsible for cybersecurity within the SME. Herefore, all surveys were directed to high-level managers employed by Dutch SMEs. This distinction is imposed by the inclusion of a separate question incorporated in the survey. A total of 134 SME-decision makers have participated within this research.

Due to the relatively sensitive nature of the information sought, safeguards were put in place to encourage participation and solicit honest responses. All surveys are conducted using a link directing the respondent to 'Qualtrics', this web-based questionnaire platform offers an

anonymous and reliable environment for taking surveys. To boost respondents' confidence, they were assured that no personal information is attached to their responses and that data collected is solely for research purposes. Safeguarding the confidentiality of the data, the raw data collected is not available to anyone other than the researcher and first supervisor.

To ensure that each respondent taking the survey represented a different organization, a review of the descriptive data is done. In this review, which incorporated size/age/sector/IT-department and responsibility-level, similar answering respondents were filtered. The consideration of different sectors, sizes, and operation-ages ensures the heterogeneity of the sample and provides robustness and generalizability to the results.

Survey distribution is done in multiple ways. Partly by using convenience sampling, when directly contacting acquaintances working as a decision-maker within a SME. Furthermore, direct contact is used in reaching SME's decision-makers of which contact details were publicly available. Moreover, respondents were reached by using online forums that provide an environment for entrepreneurs and self-employed workers, on such websites requests for taking part in this research where aimed at (translated) "Entrepreneurs, Self-employed workers, directors, and major shareholders". Examples of such online forums are: 'ZZP-Forum.nl' and 'Higherlevel.nl'. Additionally, LinkedIn and specific Facebook-groups targeting entrepreneurs and self-employed workers were used. Within these groups, the same requests as used in the online-forum webpages were made. Finally, snowball sampling is used as participants were requested to recruit other participants. Due to the fact that the survey is held in complete anonymity, it is not possible to trace back which respondent is compiled in what way. The survey distribution is done during a two-week period of time. Besides being asked to 'help with research' no other incentives to encourage participation were offered to potential respondents.

3.3 Survey content validation

To improve the validation of the questions, and hence the reliability of the results, most survey items were adopted from previously validated studies. All survey questions related to protection motivation are based on facets of constructs used in similar studies done prior, ensuring the quality and validity of the survey questions (Dang-Pham & Pittayachawan, 2015; Herath & Rao, 2009b). As prior studies, and their including surveys, are all conducted in the English language, this study translated survey questions of prior studies to the Dutch language. This was necessary due to the nature of the sample population. A five-point Likert scale is used

for all questions measuring SME's cybersecurity level and both PMT appraisal's related questions. The Likert scale is an oftentimes used instrument to quantify constructs, such as the measure of perceptions, which are not directly measurable (Gliem & Gliem, 2003). Furthermore, a combination of positively and negatively worded questions is used. A complete overview of all integrated survey questions, accompanied with the original questions as formulated in different sources, is included within this research's appendix. This section will further provide validation on the different sections used in the questionnaire. For the convenience of this section, parts of the survey are translated back to English.

Consent

For each participant, the survey first included a section requesting each participant's consent. This section provided information regarding the purpose of the survey, the aim of the research, and indicated that each survey is handled completely anonymous. This first section furthermore stated that participation is entirely voluntarily and offered the possibility to quit the survey at any time while taking part in the survey. Finally, each respondent is asked to agree to his/her answers being used during this study. Without providing their consent, the survey did not continue.

Gathering descriptive information

The survey continued with a section containing several 'general' questions regarding the SME. This section is primarily used to identify the descriptive information on each separate respondent and to test the generalizability of the sample. All questions regarding the descriptive statistics are derived from the questionnaire as provided by the DTC's 'Basisscan Cyberweerbaarheid' (2020).

The section started with a question on the number of employees working within the SME, a range of options, ranging from 1 employee up to 100-or-more employees, was provided. As discussed, the survey, aiming to reach solely the highest decision-maker responsible for digital security, included a separate question to confirm this for each respondent. Also, a question is included in which the respondent is asked to include the SME within one of twelve sector-options. This question provides information regarding the division of the sample size in different sectors. Finally, the operational age of each SME is questioned, including options ranging from 0/1-year-old organizations up to 10-year-or-older organizations.

Measuring basic security measures

The second section of the survey contained questions on the current state of cybersecurity measures within the organization. All questions are derived from the DTC's (2020) 'Basisscan Cyberweerbaarheid' and included questions on topics such as the presence or absence of '(up to date) firewalls', 'back-ups' and 'cybersecurity policy for employees' (Bernik & Prislan, 2016; Notté & Slot, 2019). More specifically, this section used the five principles as stated by the DTC (2020) as described earlier. Following these principles, a general 'level' is generated on the state of cybersecurity each respondent's SME is currently in. This level of cybersecurity is used in the statistical analysis of this study.

Following the DTC's (2020) description of the basic implementation necessary for Dutch SMEs, five principles are integrated within the survey. All questions are generated to inquire up to what extent a particular measure is included within the SME. Each question is equipped a five-point Likert scale with answering options ranging from 'this is never the case' to 'this is always the case'.

For the first principle, 'assess vulnerabilities', two questions are integrated. Tested by inquiring up to what extent the decision-maker is familiar with the software and devices within the organizations, and how frequently a back-up is made of the essential information present within the SME. The second principle, 'choose safe settings', is first tested by asking up to what extent the decision maker has implemented the use of different, complex, passwords to access company information and devices. Another question inquires whether the decision-maker has implemented the use of a two-step verification system when logging in to critical and sensitive systems. The third principle, 'make sure to update', is tested by questioning how frequently the decision-maker manages to make sure that all devices and software are updated, and how often the decision-maker is aware of the latest update available. The fourth principle, 'limit access' is tested by questioning whether the decision-maker has implemented a system in which all employees use unique secret usernames and passwords when using company devices or software. Furthermore, the decision-maker is asked whether employees are solely able to access the particular information strictly needed for their activities. The fifth principle, 'prevent viruses and malware', is tested by questioning whether the decision-maker has implemented anti-virus software on all company devices and whether this software is always up to date.

Measuring threat appraisal concepts

The next section included in the survey comprises questions related to the concepts perceived severity and perceived vulnerability, both derived from PMT's threat appraisal. All questions integrated on a five-point Likert scale ranging from 'strongly disagree' up to 'strongly agree'. The concept perceived severity is measured by including five questions related to the respondents perceived severity when it comes to cybersecurity threats. Respondents are asked how they perceive the consequences of a digital attack (Ifinedo, 2012), how they think of the importance of information security (Ifinedo, 2012), how they consider the potential loss in productivity when recovering from a cyber-attack (Herath & Rao, 2009b) and whether or not they consider loss of data or information as a serious problem to the organization (Herath & Rao, 2009b). The next five questions are related to the respondents perceived vulnerability, concerning up to what extent respondents perceive their organization as vulnerable to cyber threats. Respondents are asked to indicate the likelihood of a digital attack (Ifinedo, 2012) within their organization and are furthermore asked to what extent the information and data within the organization is perceived as vulnerable to cyber threats (Ifinedo, 2012; Williams & Joinson, 2020).

Measuring coping appraisal concepts

The final section of the survey includes questions relating to the measure of each respondent's coping appraisal. This section refers to the respondents' assessment of their ability to cope with a certain threat (Woon et al. 2005). Again, all questions integrated a five-point Likert scale ranging from 'strongly disagree' up to 'strongly agree'. This section involved questions related to the respondent's perceived response efficacy, perceived self-efficacy, and perceived response costs. The first of these three, perceived response efficacy, intended to measure the factors related to a decision-makers confidence in cybersecurity measures successfully counteract cyber threats. Questions related to this concept inquired to what extent the respondent perceives cybersecurity measures as effective within their organization (Ifinedo, 2012), and whether cybersecurity measures provide the decision-maker with a safe feeling (Dang-Pham & Pittayachawan, 2015). The second concept; perceived self-efficacy, intended to measure to what extent a respondent perceives itself capable of coping with cyber threats. Hence, the three questions related to this concept tested the respondent's perception on his/her expertise being sufficient to protect the SME (Ifinedo, 2012) and whether he or she believes

that the protection of systems and information within the company is within their control (Ifinedo, 2012; Lee et al., 2008). Finally, the questionnaire tested the respondents perceived response costs, examining to what extent the respondent perceived overhead costs and time (Ifinendo, 2012) as hindrances to implement cybersecurity measures.

3.4 Method of data analysis

All of the data is analyzed using the program *IBM SPSS Statistics 25* (IBM corp, 2017). The first part of the survey, resulting in general informative values on every particular SME's sector, age and size, is used to categorize the data and to present descriptive information about the sample data. In the results section of this study, tables are provided to further illustrate this data. This study uses a Chi-square goodness of fit test to test the representativeness of the sample (Satorra & Bentler, 2001). These tests will use an expected value derived from CBS's latest statistics on Dutch SME's (2019a).

As discussed, the second part of the survey resulted in values representing the 'level' of cybersecurity currently attained within the SME. Following the different principles as described by the DTC (2020), nine questions were part of formulating this security level. To generate a 'level' of cybersecurity for each respondent, a new scale is created using the compute variable function in SPSS (IBM corp, 2017). This scale combined the answers on the nine different questions and resulted in a new variable. The variable 'Cybersecurity Level' provided data indicating the cybersecurity 'level' each respondent's SME is currently on. The higher the score, the more cybersecurity measures are generally implemented. A distinction on the scales measuring cybersecurity measures is made in measuring different components on occurrence. Regarding the different cybersecurity measures, respondents answered on a scale from 1 (never implemented) to 5 (always implemented). A 'perfect' score is hence reached within an organization stating that all tested cybersecurity measures are always implemented. The lowest possible score is attained within an organization that states to never have any of the tested aspects implemented. Following the research hypotheses, this scale is used to statistically test for a relationship with the stated concepts as derived from PMT.

As stated, the final part of the survey included the questions regarding the different concepts as formulated in the protection motivation theory (Rogers, 1975). Derived from both the threat and coping appraisal, five concepts that influence protection motivation are derived. Each

concept containing the values as generated from the questions included within the survey. To analyze the values of each concept, scales are created. Hence, the perceived severity scale included all perceived severity related questions. The same is done for perceived vulnerability, perceived response efficacy, perceived self-efficacy and perceived response costs. To test the internal consistency among the items included within the different scales, this study used Cronbach's alpha tests. This tests' results showed up to what extent for all questions the same construct is measured and whether or not a correlation is found among these items (Gliem & Gliem, 2003). This study followed Cronbach's alpha's highest 'if item deleted' scores, hence acquiring the highest possible internal consistency for each created variable.

Prior to testing the formulated hypotheses, this study will conduct a test for multicollinearity, linearity, normality and potential outliers in the data. A one-way ANOVA is conducted to compare the effect of the protection motivation factors on the level of cybersecurity implementation (Stoline, 1981). Following the hypotheses as formulated in this research, the relation between the 'basic' cybersecurity level scale and each PMT-concept is tested. This relation is measured by using regression analysis. A regression analysis provides a set of statistical processes that allow an estimation of the relationship between a dependent variable and one or more independent variables (Rubinfeld, 2011). In other words, a relationship between the outcome variable, in this case the cybersecurity level for each SME, and different predictors, the different PMT concepts. Using this statistical analysis allowed to both generate an overall relationship and indicate the relationship between the dependent variable and each separate independent variable. Hence testing the hypotheses and providing an answer to the stated research question.

4 Data Analysis and Results

4.1 Descriptive statistics

A total of 208 respondents 'clicked' on the anonymous link and hence started the survey. Within this number, a total of 164 respondents were verified to give their consent for the use of their data within this study and to complete all survey-questions. Furthermore, organizations with exactly the same descriptive statistics were filtered. To make sure the survey is completed by the highest decision-maker regarding cybersecurity within each SME, the survey included a selection question. This question specifically inquired the respondents' responsibility regarding cybersecurity issues. On this question, 15 respondents replied to have 'nothing to do with cybersecurity', and 15 other respondents replied to 'have something to do with cybersecurity but indicated to not be the final decision-maker'. This left a sample size of 134 Dutch SME decision-makers fully responsible for the cybersecurity within their organization. As this study researches a relation between the implementation of cybersecurity measures, and protection motivation factors as perceived by the final decision-maker within a Dutch SME, this study will continue to use the data derived from these 134 respondents. This section will further present the descriptive information on the sample size.

Table 1
Descriptive Statistics

Variables	**N**	**%**
Number of Employees		
1 employee	56	41.8
2 employees	17	12.7
3-4 employees	19	14.2
5-9 employees	20	14.9
10-19 employees	5	3.7
20-49 employees	6	4.5
50-99 employees	5	3.7
100-250 employees	6	4.5
Primary Sector		
Industry & Energy	3	2.2
Construction	7	5.2
Trade, Transport & Catering	17	12.7
Information & Communication	12	9
Financial Services	10	7.5
Rental & Property trade	6	4.5
Business Services	42	31.3
Government & Care	8	6
Culture & Recreation	7	5.2

Other Services	22	16.4
Organization Age		
0-1 year	10	7.5
1-2 years	15	11.2
3-5 years	25	18.7
6-10 years	29	21.6
10+ years	55	41

Sample size

Regarding SME sizes, a total of 56 respondents reported to represent a self-employed person, this represents 41.8% of the total sample size. Hence, 78 respondents represent organizations in which 2 or more employees are employed, representing 58.2% of the total sample size. More specifically, 17 respondents (12.7%) represent organizations with 2 employees, 19 respondents (14.2%) represent organizations with 3-4 employees, 20 respondents (14.9%) represent organizations with 5-9 employees, 5 respondents (3.7%) represent organizations with 10-19 employees, 6 respondents (4.5%) represent organizations with 20-49 employees, 5 respondents (3.7%) represent organizations with 50-99 employees and 6 respondents (4.5%) represent organizations with 100-250 employees. An overview of these results is provided in table 1. Following the latest data on Dutch SMEs from CBS (2019a), table 2 presents the expected results regarding sample size. Given the fact that, in 2019, almost 75% of the complete Dutch SME sector consisted of self-employed organization, about 100 self-employed organizations was expected. Due to the relatively large mismatch between observed and expected value of 'self-employed' organizations, no Chi-Square goodness of fit test is conducted.

Table 2
Expected Results Size variable

SME Size	Observed	Expected	Residual
Self-Employed	56	100	44
2-10 Employees	56	27	29
10-50 Employees	11	5	-6
50-250 Employees	11	1	-10

Sample sector

The sample size includes organizations representing different primary sectors. Results show that respondents are included in a total of 10 different sectors. The largest group of respondents, representing 31.3% of the total sample, indicated to be part of the 'business services' sector. This sector is followed by respectively 'other services' (16.4%) and the 'Trade, Transport &

Catering' sector (12.7%). An overview of all results regarding the SME's sectors, is provided in table 1. The division of sectors used in this research is consulted from the DTC (2020). The fact that a large portion of the sample size indicated to be primarily be part of 'other services' made it hard to test the generalizability of the sample on sector. Furthermore, CBS (2019a) makes use of a slightly different sector-mapping, making it difficult to statistically test generalizability.

Sample age

Finally, respondents are divided in different age categories. Within this division, 55 respondents, the biggest portion of the sample size, indicated to represent an organization active for more than 10 years (41%). This group is followed by 29 respondents (21.6%) representing an organization 6-10 years of age. Then, 25 respondents (18.7%) represent organizations 3-5 years of age and the final 25 respondents (18.7%) represent organizations active for less than 3 years. Table 1 presents the division in age regarding the entire sample size. To test how the sample generalizes in terms of the distribution of SME-age, a Chi-Square goodness of fit test is conducted. The test is conducted by using an expected value derived from CBS (2019a); in these data 'smaller than 3' represents 20.9%, '3-5' represents 14.5%, '6-10' represents 26.7%, and '10+' represents 37% of the total number of SMEs. A *p* value of .217 indicates that the distribution of the observed results is similar to the distribution as stated by CBS (Parke, 2012). Test and results are included in Table 3 and 4.

Table 3
Results Chi-Square Age variable

SME Age	Observed	Expected	Residual
Less than 3 years	25	28	-3
3-5 years	25	19	6
6-10 years	29	37	-8
10+ years	55	50	5

Table 4
Chi-Square goodness of fit test

	Value
Chi-Square	4.6
Asymp. Sig.	.217

4.2 Scale creation and reliability

Different scales were created to test the dependent and different independent variables. Prior to the creation of these scales, a Cronbach's Alpha test is conducted to test the reliability of the created scales. Following Cronbach's Alpha's 'if items deleted' scores, the highest possible reliability is reached for each variable. For the independent variable 'perceived severity' a .003 higher reliability score could have been reached by deleting one item. However, due to the minor increase in reliability, this item was not deleted. Generally, the Cronbach's Alpha scores are showing a 'good' or 'excellent' reliability (George & Mallery, 2003). Results of each variables' Cronbach's Alpha, the number of items per variable, and the number of items deleted per variable, are provided in table 5.

Table 5

Cronbach's Alpha results

Variable	Cronbach's Alpha	N of Items	Items deleted
Cybersecurity Level	.820	8	1
Perceived Severity	.857	5	0
Perceived Vulnerability	.800	5	0
Perceived Response Efficacy	.634	2	1
Perceived Self Efficacy	.832	3	0
Perceived Response Costs	.706	3	0

4.3 Testing general assumptions

First, multicollinearity among the different variables is tested by analyzing correlations among the independent variables. No correlation above .7 is found among the different independent variables, this is a first indication multicollinearity is not present. This result was confirmed by the collinearity statistics. All independent variables scored above .72 on tolerance and indicated a maximum VIF score of 1.38. The high tolerance scores and the low VIF numbers indicate that changes in one variable are only to a very limited extend associated with shifts in other variables (Mansfield & Helms, 1982),

The normal P-P plot indicated a reasonably close following of the line of best fit. Only little deviation is seen following this line, indicating little deviation from normality is found. Furthermore, the sample showed one case's residual value to be -3.2. By using Cook's Distance, the influence of a particular case on the outcome of the analysis is measured. Cook's

distance, in this case .146, indicates that this individual case is not having a significant influence on the ability to predict the outcome of the research model (Kim & Storter, 1996).

The distribution of the results presented in a scatterplot shows generally clustered results, this meets the assumption of linearity. A few outliers are indicated in the scatterplot, however, given the sample size, this number of outliers is neglectable. No systematic pattern is found within the distribution of the dots. To further test for outliers, Mahalanobis Distances are used. The Mahalanobis Distances, as created in a multiple regression analysis, are compared to a Chi-Square distribution with the same degrees of freedom. The degrees of freedom correspond with the number of independent variables. A *p*-value of the right-tail of the Chi-Square distribution is computed. No multivariate outliers are present as no values of less than .001 were shown in the probability variable (De Maesschalck et al., 2000). The smallest found variable showed a value of .017, hence, no indication is found to remove any outliers. Tables on linearity, multicollinearity and normality tests are included in this study's appendix.

4.4 Regression Analysis

To test the research model, a linear regression analysis is conducted. This analysis shows what portion of the variance on the dependent variable, cybersecurity level, is explained by the research model. In this test the model includes all 5 independent variables at the same time. Results of this test show an adjusted *R* squared of .546. This suggest that 54.6% of the variance in cybersecurity level is explained by a combination of perceived severity, perceived vulnerability, perceived response efficacy, perceived self-efficacy and perceived response costs. A one-way between subject ANOVA is conducted to compare the effect of the protection motivation factors on the level of cybersecurity implementation. There is a significant effect of the independent variables on the dependent variable at the $p<.05$ level [$F(5, 128)= 32.99$, $p = .00$].

Table 6
Model Overview *

R	R Square	Adjusted R Square	Std. Error of the estimate
.750**	.563	.546	3.84

*Dependent Variable: Cybersecurity Level

** Predictors: (Constant), Perceived Response Costs, Perceived Vulnerability, Perceived Self- Efficacy, Perceived Severity, Perceived Response Efficacy

The standardized coefficients and the significance for the different independent variables are presented in table 7. These coefficients show us that perceived severity, perceived response efficacy and perceived self-efficacy show a significant unique contribution to the prediction of the implementation of cybersecurity measures. The variable perceived response costs indicated a negative significant contribution to the prediction of the implementation of cybersecurity. The positive contribution indicated by the variable perceived vulnerability turned out to be insignificant.

Table 7
Standardized Coefficients and Part Correlation for independent variables.

Variable	Standardized Coefficients	Sig.	Part Correlation	Part squared
Perceived Severity	.394	.000	.245	.060
Perceived Vulnerability	.035	.593	.048	.000
Perceived Response Efficacy	.270	.000	.212	.045
Perceived Self-Efficacy	.312	.000	.295	.087
Perceived Response Cost	-.170	.008	-.126	.016

Table 7 furthermore presents the part correlations for each independent variable. When squared, the part correlation provides an indication of the contribution of each individual variable to the total *R* squared. Hence, generating an overview of what percentage of the total variance in the outcome is uniquely explained by that specific variable, and how much *R* squared would drop if this variable is removed from the model. In this case, perceived severity uniquely represents 6% of the generated R squared. The part correlation solely represents the unique contribution of each indicated variable the total of the five variables and does not equal the total R squared, this is explained by the inclusion of shared variance.

5 Discussion

5.1 Main findings

By integrating PMT, this study proposed and validated a research model designed to enrich the understanding of the relationship between the protection motivation and the implementation of cybersecurity measures in the Dutch SME sector. The study's results show that a significant amount of variance in the proposed dependent variable is explained by the model's independent variables. Although previous research has explored PMT in relation to a range of security behaviors (Boss et al., 2015), this study is the first to use this approach in the context of SME decision makers and the implementation of basic cybersecurity measures within an organizational setting. By analyzing a relationship between currently implemented security measures and different PMT factors, this study attempted to address the explanation of security behavior. Herefore, going further than most related studies predicting security intentions (Boss et al., 2015). Furthermore, by using PMT as a theory to explain behavior on a managerial level, this study used a different point of view in explaining security-related behaviors within organizations than most prior studies.

The study's results show that a statistically significant relationship with moderate strength (Frost, 2013) is found between the different independent variables and the dependent variable. About 54% of the total variance in the dependent variable is explainable by a combination of the five different independent variables. Given the fact that this study attempted to explain human behavior, the research model explaining a variance of above 50% is generally seen as decent measure (Frost, 2013). Regarding the formation of SME's decision makers' threat appraisal, the results indicate that those who consider the consequences of a cyber related threat to be more severe to their organization are more likely to implement a higher level of cybersecurity measures. However, decision makers that have a greater perception on their organization's vulnerability did not show a significantly greater cybersecurity level. As per the coping appraisal related concept, the results showed a statistically significant effect for all three components. This section will further discuss the unique significance of the different independent variables included in the research model.

Perceived severity

Derived from PMT's threat appraisal, the concept perceived severity is found to have a significant positive effect on the implementation of cybersecurity measures. This result states

that, for a decision maker, the assessment of the consequences of a cyberbreach plays an important role in making the decision to implement cybersecurity measures. The significant relationship affirms the first stated hypothesis.

Perceived vulnerability

Although a positive relationship between a decision maker's perceived vulnerability and the implementation of cybersecurity measures is found, this relationship turned out to be insignificant. The direction of the relationship is consistent with prediction and prior studies (Herath & Rao, 2009b, Ifinedo, 2012), the strength of the relationship however is insignificant to confirm the stated hypothesis. This result indicates that the assessment of the probability of threatening events happening does not have a significant effect on the implementation of cybersecurity measures for decision makers within the Dutch SME sector. This result is possibly explained by decision makers having too little knowledge on the vulnerability of their organization. In this sense decision makers might lack the awareness on cyber threats to comprehend the danger their organization is potentially in (Lopez-Nicolas & Soto-Acosta, 2010; Mulligan & Schneider, 2011). Another plausible reason for this result may be due to sample composition and research design. The insignificance of this correlation does however indicate that the relationship between perceived vulnerability and the implementation of cybersecurity is not determined by the level of cybersecurity implementations. The results show that a higher level of cybersecurity implementation does not imply a lower level of perceived vulnerability.

Perceived Response Efficacy

Confirming the third stated hypothesis, response efficacy is found to have a significant positive relationship with the implementation of a basic level of cybersecurity measures. Hence, the confidence SME's decision makers have in security measures to prevent organizational losses and generate a feeling of safety is found to have a positive relationship with the implementation of cybersecurity measures.

Perceived Self-Efficacy

The independent variable perceived self-efficacy, emphasizing a decision maker's judgement regarding his or her capabilities to implement adequate cybersecurity measures, showed a significant positive relationship with the implementation of cybersecurity measures. This confirms the fourth stated hypothesis. Self-efficacy showed to generate the largest part-

correlation of all independent variables, this indicates the value of this variable in the general correlation.

Perceived Response Costs

Finally, perceived response costs generated a significant negative relationship with the implementation of cybersecurity measures. Hence, for decision makers within the Dutch SME sector, the perception of high costs in terms of time, effort, or monetary, to implement cybersecurity measures is found to have a negative relationship with the implementation of cybersecurity measures.

5.2 Limitations

This study has several limitations that should be considered. First, regarding the validity of this study, it is possible that participants might have provided "socially desirable responses" (Podsakoff et al., 2003). Socially desirable responses potentially influenced both respondent's cybersecurity level and the measured PMT concepts. Mainly regarding respondent's cybersecurity level, this is enhanced by the relatively sensitive nature of the subject cybersecurity. Furthermore, it is possible that some of the measure's items used in the questionnaire have been misinterpreted by respondents. The answers obtained would hence have negatively influenced the data analysis, resulting in implications for this study's internal validity (Roe & Just, 2009).

Regarding the generalizability of the sample, the results show that mainly the descriptive 'company size' shows a relatively large total deviation from the expected values. This deviation is primarily caused by the relatively low number of self-employed SMEs within the sample size. The group 'self-employed' SME's represents the largest group within the sample size but does not reach the quantity predicted by CBS (2019a). CBS does not provide exact numbers on the amount of active and inactive organizations; hence the number of 'self-employed' organizations possibly contains a large amount of relatively inactive organizations.

Furthermore, the sample size is not totally random. Regarding the external validity of this study, the sample size to a large extent met the CBS's (2019a) data on SME-population, a larger sample size would however provide more statistical power and performance. The strict distinction in reaching responsible decision-makers, and the given that respondents tend to be

reluctant in discussing their cybersecurity measures, at times caused a slight hindrance to the respondent gathering process.

Regarding the reliability of this study, it has to be noted that the cybersecurity space is a rapidly evolving sector, both regarding the evolution of threats and security measures. Cybersecurity is a 'hot-topic' in which conditions constantly change, this may cause problems to the reproducibility of this study. Furthermore, the measured 'level' of cybersecurity in this study is based on 8 questions. Although all principles as stated by the DTC (2020) are incorporated within this construct, some respondents might have 'missed' security measures which they actually have implemented. This could have resulted in lower overall cybersecurity scores for some respondents. This study analyzed protection motivational factors as formulated in the protection motivation theory (Rogers, 1975) and did not take other environmental conditions into account. Other conditions such as deterrence, facilitating conditions, and social influence, potentially influence protection motivation (Herath & Rao, 2009b).

5.3 Suggestions for future work

Descriptive statistics for this study were solely used to provide an overview of the sample population, hence no statistical analysis is done using these variables as predictors within the research model. Future research should tend to obtain a larger sample size and should investigate whether descriptive statistics influence the variables and outcome of the research model.

This study provides a validated measure that investigates the influence of different protection motivation factors on the implementation of cybersecurity measures. Future research could however further examine the relationship between the constructs within the survey measure and examine the relationship between these constructs and the implementation of cybersecurity measures. Furthermore, additional research is necessary regarding the different protection motivation constructs and the implementation of specific cybersecurity measures. By testing specific security measures or using a more inclusive typology of basic cybersecurity measures, more knowledge will be generated on the influences of protection motivation factors on specific cybersecurity measures. This way, future research can better provide effective guidance to decision makers in organizational settings. More knowledge and more precise advice will increase the likelihood of attaining a cybersecure SME sector.

5.4 Conclusion

This study provides a foundation that can be used to further examine the relationship between protection motivation and the implementation of security measures and further research on the implementation of cybersecurity measures from a top-level perspective. To enrich the knowledge in the area, this research drew from a relevant behavioral theory with PMT. By using different variables derived from the protection motivation theory, this research examined the relationship between protection motivation and the implementation of cybersecurity measures within the Dutch SME sector. A survey is conducted among SME's final decision makers regarding cybersecurity implementation.

The study hence provides a first step in understanding the different factors that influence SME's decision makers in implementing cybersecurity measures. Overall, four out of five stated hypotheses were uniquely found to significantly influence the implementation of cybersecurity measures and the general correlation of the independent variables indicated to be significant. Herefore, this study concludes that protection motivation factors are indeed related to the implementation of cybersecurity measures within the Dutch SME sector. More specifically, this study's findings predict that factors related to perceived severity, perceived self-efficacy, perceived response efficacy and perceived response costs have a direct relationship with the level of implemented cybersecurity measures. The results of this study should be taken into account when generating, implementing or adjusting security awareness campaigns, public-private partnerships, and other initiatives meant to increase the cyber resilience in the Dutch SME sector.

6 References

Accenture (2019). The Cost of Cybercrime. *Research conducted by Ponemon Institute LLC*. Retrieved from: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Al-Ghaith, W. (2016). Extending protection motivation theory to understand security determinants of anti-virus software usage on mobile devices. *International Journal of Computers*, *10*, 125-138.

Allianz (2019) *Oktober*. MKB'ers onderschatten gevaren cybercriminaliteit. *Research conducted by Ipsos*. Retrieved from: https://www.allianz.nl/algemeen/nieuws/nieuws2019/mkbers-onderschatten-gevaren-cybercriminaliteit

Alshboul, Y., & Streff, K. (2015). Analyzing Information Security Model for Small-Medium Sized Businesses.

Alwanain, M. I. (2019). Effects of User-Awareness on the Detection of Phishing Emails: A Case Study. doi: https://doi.org/10.14569/IJACSA.2019.0101046

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS quarterly*, *34*(3), 613-643. doi: https://doi.org/10.2307/25750694

Asllani, A., White, C. S., & Ettkin, L. (2013). Viewing cybersecurity as a public good: The role of governments, businesses, and individuals. *Journal of Legal, Ethical and Regulatory Issues*, *16*(1), 7.

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*.

Bell, S. (2017). Cybersecurity is not just a'big business' issue. *Governance Directions*, *69*(9), 536.

Bernik, I., & Prislan, K. (2016). Measuring information security performance with 10 by 10 model for holistic state evaluation. *PloS one*, *11*(9), e0163050.

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly (MISQ)*, *39*(4), 837-864. doi:https://doi.org/10.25300/MISQ/2015/39.4.5

Bossong, R., & Wagner, B. (2017). A typology of cybersecurity and public-private

Partnerships in the context of the EU. *Crime, Law and Social Change*, *67*(3), 265-288.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548. doi: https://doi.org/10.2307/25750690

Carr, M. (2016). Public–private partnerships in national cybersecurity strategies. *International Affairs*, *92*(1), 43-62. doi: https://doi.org/10.1111/1468-2346.12504

CBS (2019a) MKB-kerncijfers. Retrieved from: https://mkbstatline.cbs.nl/#/MKB/nl/navigatieScherm/thema?themaNr=48042

CBS (2019b) Meer 'kleine' mkb-bedrijven. Retrieved from: https://www.cbs.nl/nl-nl/nieuws/2019/31/meer-kleine-mkb-bedrijven

Centraal Beheer (2018) *November*. Cybersecurity, Opvallende uitkomsten cyberonderzoek. *Conducted by Ipsos.*

Chenoweth, T., Minch, R., & Gattiker, T. (2009, January). Application of protection motivation theory to adoption of protective technologies. In *2009 42nd Hawaii International Conference on System Sciences* (pp. 1-10). IEEE.

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & security*, *30*(8), 719-731. doi:https://doi.org/10.2139/ssrn.2339821

Crossler, R. E. (2010, January). Protection motivation theory: Understanding determinants to backing up personal data. In *2010 43rd Hawaii International Conference on System Sciences* (pp. 1-10). IEEE. doi: https://doi.org/10.1109/HICSS.2010.311

CSIRT-DSP (2019, Maart). CSIRT-DSP. *Ministerie van Economische Zaken en Klimaat*. RFC2350. Versie 1.1. Retrieved from: https://csirtdsp.nl/sites/default/files/2019-03/20190318_CSIRT%20DSP_RFC2350v1.1.pdf

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security*, *48*, 281-297. doi:https://doi.org/10.1016/j.cose.2014.11.002

De Maesschalck, R., Jouan-Rimbaud, D., & Massart, D. L. (2000). The mahalanobis distance. *Chemometrics and intelligent laboratory systems*, *50*(1), 1-18.

DeNardis, L. (2007). A history of internet security. In *The history of information security* (pp.

681-704). Elsevier Science BV. doi: https://doi.org/10.1016/B978-044451608-4/50025-0

Digital Trust Center (2020). De 5 basisprincipes van veilig digitaal ondernemen. Retrieved from:https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen

Dykstra, J. (2015). *Essential cybersecurity science: build, test, and evaluate secure systems*. " O'Reilly Media, Inc."

European Commission (2019). *What is an SME?* Retrieved from: https://ec.europa.eu/eurostat/web/structural-business-statistics/structural-business-statistics/sme

European Commission (2019b, March). *The Cybersecurity Act strengthens Europe's cybersecurity.* Retrieved from: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-act-strengthens-europes-cybersecurity.

Fischer, E. A. (2014). Cybersecurity issues and challenges: in brief.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of applied social psychology*, *30*(2), 407-429.

Frost, J. (2013). Regression analysis: How do I interpret R-squared and assess the goodness-of-fit. *The Minitab Blog*, *30*.

Gafni, R., & Pavel, T. (2019). The invisible hole of information on SMB's cybersecurity. *Online Journal of Applied Knowledge Management (OJAKM)*, *7*(1), 14-26. doi: https://doi.org/10.36965/OJAKM.2019.7(1)14-26

George, D., & Mallery, M. (2003). Using SPSS for Windows step by step: a simple guide and reference.

Gliem, J. A., & Gliem, R. R. (2003). Calculating, interpreting, and reporting Cronbach's Alpha reliability coefficient for Likert-type scales. Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education.

Grapperhaus, F (2019) Brief regering; Voortgang integrale aanpak cybercrime – Naar een veiliger samenleving. *Commissie Justitie en Veiligheid.*

Guttman, B., & Roback, E. A. (1995). *An introduction to computer security: the NIST handbook*. Diane Publishing. doi: https://doi.org/10.6028/NIST.SP.800-12

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cybersecurity, and the Copenhagen School. *International studies quarterly*, *53*(4), 1155-1175. doi:https://doi.org/10.1111/j.1468-2478.2009.00572.x

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security

behavior: a protection motivation theory perspective. *Information Systems Management*, *33*(1), 2-16.

Herath, T., & Rao, H. R. (2009a) Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125.

Hiscox (2019) *Hiscox cyber readiness report 2019.* Retrieved from: https://www.hiscox.nl/sites/www.hiscoxnl.com/files/filedepot/Hiscox_cyber_readiness_report.pdf. doi: https://doi.org/10.1016/S1353-4858(19)30057-1

IBM Corp. Released 2017. IBM SPSS Statistics for Macintosh, Version 25.0.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95. doi:https://doi.org/10.1016/j.cose.2011.10.007

Ilvonen, I., & Virtanen, P. (2013). Preparing for cyber threats in companies with information security policies. *Information Warfare and Security*, 120. doi:https://doi.org/10.4018/ijcwt.2013100103

Kim, C., & Storer, B. E. (1996). Reference values for Cook's distance. *Communications in Statistics-Simulation and Computation*, *25*(3), 691-708. doi:https://doi.org/10.1080/03610919608813337

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & security*, *25*(4), 289-296. doi:https://doi.org/10.1016/j.cose.2006.02.008

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online Protection behavior. *Behavior & Information Technology*, *27*(5), 445-454. doi:https://doi.org/10.1080/01449290600879344

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives'decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177-187.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information management & computer security*. doi:https://doi.org/10.1108/09685220210424104

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, *37*(12), 1049-1092. doi: https://doi.org/10.1108/MRR-04-2013-0085

Lopez-Nicolas, C., & Soto-Acosta, P. (2010). Analyzing ICT adoption and use effects on knowledge creation: An empirical investigation in SMEs. *International Journal of Information Management*, *30*(6), 521-528.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology*, *19*(5), 469-479.

Mansfield, E. R., & Helms, B. P. (1982). Detecting multicollinearity. *The American Statistician*, *36*(3a), 158-160. doi: https://doi.org/10.2307/2683167

Milne, S., Orbell, S., & Sheeran, P. (2002). Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British journal of health psychology*, *7*(2), 163-184. doi: https://doi.org/10.1348/135910702169420

MKB-Nederland (2017) *MKB-ondernemer vaakst slachtoffer van malware.* Retrieved from: https://www.mkb.nl/nieuws/mkb-ondernemer-vaakst-slachtoffer-van-malware

MKB-Nederland (2020) *Officiele website MKB-Nederland.* retrieved from: https://www.mkb.nl/.

North Atlantic Treaty Organization (2019) Increasing NATO's ability to respond to cybersecurity concerns. *Research Report, XXIX.*

NCSA (2018) Nederlandse Cybersecurity Agenda. Nederland Digitaal veilig. *Ministerie van Justitie en Veiligheid.*

NCTV (2020) Nationaal Crisisplan Digitaal. Nationaal Coördinator Terrorisme en Veiligheid. *Ministerie van Justitie en Veiligheid*.

NOS (2019, December). *Universiteit Maastricht kampt met ransomware-aanval*. Derived from: https://nos.nl/artikel/2316120-universiteit-maastricht-kampt-met-ransomware-aanval.html

Notté, R. & Slot, L (2019). Hoe cyber-secure is het mkb? *Nulmeting cybersecurity in het mkb*. De Haagse Hogeschool. Retrieved from: https://www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/lectoraten/cybersecurity-in-het-mkb/infographic-nulmeting-cybersecurity-mkb.pdf

Osborn, E. (2015). Business versus technology: Sources of the perceived lack of

cybersecurity in SMEs.

Parke, C. S. (2012). *Essential first steps to data analysis: Scenario-based examples using SPSS*. Sage Publications. doi: https://doi.org/10.4135/9781506335148

Paulsen, C. (2016). Cybersecuring small businesses. *Computer*, *49*(8), 92-97. doi:https://doi.org/10.1109/MC.2016.223

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of applied psychology*, *88*(5), 879. doi: https://doi.org/10.1037/0021-9010.88.5.879

Posthumus, S., & von Solms, R. (2004, November). A responsibility framework for information security. In *Working Conference on Integrity and Internal Control in Information Systems* (pp. 205-221). Springer, Boston, MA.

Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management*, *11*(4), 489-510.

Rijksoverheid (2018) Digital Trust Center maakt veilig digitaal ondernemen makkelijker. Retrieved from: https://www.rijksoverheid.nl/actueel/nieuws/2018/06/08/digital-trust-center-maakt-veilig-digitaal-ondernemen-makkelijker

Rijksoverheid (2018b) Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) voor Digitale Dienstverleners. *Ministerie van Economische Zaken en Klimaat*.

Roe, B. E., & Just, D. R. (2009). Internal and external validity in economics research: Tradeoffs between experiments, field experiments, natural experiments, and field data. *American Journal of Agricultural Economics*, *91*(5), 1266-1271.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, *91*(1), 93-114. doi:https://doi.org/10.1080/00223980.1975.9915803

Rubinfeld, DL (2011). National Research Council. *Reference manual on scientific evidence.* National Academies Press.

Ryan, J. J. (2004). Information security tools and practices: what works?. *IEEE Transactions on Computers*, *53*(8), 1060-1063. doi: https://doi.org/10.1109/TC.2004.45

Sangani, N. K., & Vijayakumar, B. (2012). Cybersecurity scenarios and control for small and medium enterprises. *Informatica Economica*, *16*(2), 58.

Satorra, A., & Bentler, P. M. (2001). A scaled difference chi-square test statistic for moment

structure analysis. *Psychometrika*, *66*(4), 507-514. doi:https://doi.org/10.2139/ssrn.199064

Scully, T. (2014). The cybersecurity threat stops in the boardroom. *Journal of business continuity & emergency planning*, *7*(2), 138-148.

Shojaifar, A., Fricker, S. A., & Gwerder, M. (2018). Elicitation of SME Requirements for Cybersecurity Solutions by Studying Adherence to Recommendations. In *REFSQ Workshops*.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*. doi: https://doi.org/10.1108/09685220010371394

Siponen, M. T. (2001). Five dimensions of information security awareness. *SIGCAS Computers and Society*, *31*(2), 24-29.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1982). Why study risk perception?. *Risk analysis*, *2*(2), 83-93. doi: https://doi.org/10.1111/j.1539-6924.1982.tb01369.x

Stoline, M. R. (1981). The status of multiple comparisons: simultaneous estimation of all pairwise comparisons in one-way ANOVA designs. *The American Statistician*, *35*(3), 134-141. doi: https://doi.org/10.2307/2683979

Tawileh, A., Hilton, J., & McIntosh, S. (2007). Managing information security in small and medium sized enterprises: A holistic approach. In *ISSE/SECURE 2007 Securing Electronic Business Processes* (pp. 331-339). Vieweg.

Tarter, A. (2017). Importance of cybersecurity. In *Community Policing-A European Perspective* (pp. 213-230). Springer, Cham. doi: https://doi.org/10.1007/978-3-319-53396-4_15

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138-150. doi:https://doi.org/10.1016/j.cose.2016.02.009

Valli, C., Martinus, I. C., & Johnstone, M. N. (2014). Small to medium enterprise cybersecurity awareness: an initial survey of Western Australian business.

Verizon (2019) Data Breach Investigations Report. Retrieved from: https://enterprise.verizon.com/en-gb/resources/reports/dbir/. doi: https://doi.org/10.1016/S1361-3723(19)30060-0

Von Solms, R., & Van Niekerk, J. (2013). From information security to cybersecurity. *Computers & security*, *38*, 97-102.

doi:https://doi.org/10.1016/j.cose.2013.04.004.

Williams, E. J., & Joinson, A. N. (2020). Developing a measure of information seeking about phishing. *Journal of Cybersecurity*, *6*(1), tyaa001. doi:https://doi.org/10.1093/cybsec/tyaa001

Witte, K. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of health communication*, *1*(4), 317-342. doi:https://doi.org/10.1080/108107396127988

Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security. *ICIS 2005 proceedings*, 31.

Yost, J. R. (2007). A history of computer security standards. In *The History of Information Security* (pp. 595-621). Elsevier Science BV. doi:https://doi.org/10.1016/B978-044451608-4/50021-3

Zec, M., & Kajtazi, M. (2015, September). Examining how it professionals in smes take decisions about implementing cybersecurity strategy. In *ECIME2015-9th European Conference on IS Management and Evaluation: ECIME 2015*(p. 231). Academic Conferences and publishing limited.

7 Appendices

7.1 Appendix A: Questionnaire

Descriptive Measures

1. Hoeveel werknemers werken er in het bedrijf waar je werkt?
    - 1 persoon (ZZP)
    - 2 personen
    - 3-4 personen
    - 5-9 personen
    - 10-19 personen
    - 20-49 personen
    - 50-99 personen
    - 100 personen of meer

2. Regelt u zelf binnen het bedrijf de zaken rondom digitale veiligheid of bent u hiervoor (eind)verantwoordelijk?
    - Ja ik ben eindverantwoordelijk
    - Ja ik regel deze zaken (niet eindeverantwoordelijk maar hou me er wel mee bezig)
    - Nee, geen van beiden

3. Heeft het bedrijf een eigen IT-afdeling/ eigen IT-medewerkers?
    - Ja,
    - Nee wij hebben dit uitbesteed
    - Nee op een andere manier

4. Binnen welke branche bent u vooral werkzaam?
    - Landbouw, bosbouw en visserij
    - Nijverheid (geen bouw) en energie
    - Bouwnijverheid
    - Handel, vervoer en horeca
    - Informatie en communicatie
    - Financiële dienstverlening
    - Verhuur en handel van onroerend goed
    - Zakelijke dienstverlening
    - Overheid en zorg
    - Cultuur en recreatie
    - Overige diensten
    - Weet niet

5. Hoe lang bestaat het bedrijf al?
    - 0-1 jaar, 1-2 jaar, 3-5 jaar, 6-10 jaar, Langer dan 10 jaar

Current cybersecurity level

Make an assessment of vulnerabilities (2 times)

6. Ik weet precies welke apparatuur en software binnen mijn bedrijf worden gebruikt.
    - Dit is nooit het geval
    - Dit is zelden het geval
    - Dit is soms het geval
    - Dit is vaak het geval
    - Dit is altijd het geval

7. Er wordt regelmatig een kopie gemaakt van alle belangrijke informatie binnen mijn bedrijf.
    - Dit is nooit het geval
    - Dit is zelden het geval
    - Dit is soms het geval
    - Dit is vaak het geval
    - Dit is altijd het geval

Use safe setttings (2 times)

8. Om apparaten en bedrijfsgegevens te gebruiken (in de cloud, e-mail, social media accounts) zijn verschillende, moeilijk te raden en complexe wachtwoorden ingesteld
    - Dit is nooit het geval
    - Dit is zelden het geval
    - Dit is soms het geval
    - Dit is vaak het geval
    - Dit is altijd het geval

9. Om in te loggen op gevoelige of kritieke systemen maken wij binnen ons bedrijf gebruik van niet alleen een gebruikersnaam en wachtwoord, maar ook een extra beveiliging via bijvoorbeeld een code op een telefoon (tweefactor authenticatie).
    - Dit is nooit het geval
    - Dit is zelden het geval
    - Dit is soms het geval
    - Dit is vaak het geval
    - Dit is altijd het geval

Make sure to update (2 times)

10. Alle apparatuur en software binnen mijn bedrijf is voorzien van de laatste updates.
    - Dit is nooit het geval
    - Dit is zelden het geval
    - Dit is soms het geval
    - Dit is vaak het geval

- Dit is altijd het geval

11. Ik ben op de hoogte van de laatste beschikbare updates en installeer deze direct
  - Dit is nooit het geval
  - Dit is zelden het geval
  - Dit is soms het geval
  - Dit is vaak het geval
  - Dit is altijd het geval

Limit Access (2 times)

12. Ik en al mijn medewerkers/collega's hebben een eigen geheime gebruikersnaam en wachtwoord voor het gebruik van bedrijfsapparatuur en software.
  - Dit is nooit het geval
  - Dit is zelden het geval
  - Dit is soms het geval
  - Dit is vaak het geval
  - Dit is altijd het geval

13. Mijn medewerkers/collega's kunnen alleen bij de informatie die zij nodig hebben voor hun werkzaamheden
  - Dit is nooit het geval
  - Dit is zelden het geval
  - Dit is soms het geval
  - Dit is vaak het geval
  - Dit is altijd het geval

Prevent viruses and malware (1 time)

14. Op alle bedrijfsapparatuur is antivirussoftware aanwezig en up-to-date.
  - Dit is nooit het geval
  - Dit is zelden het geval
  - Dit is soms het geval
  - Dit is vaak het geval
  - Dit is altijd het geval

Threat Appraisal

Perceived severity (5 times):

Having someone successfully attack and damage my computer (at work) is:
Likert scale 1/7 harmless 1 harmful 7 (ifinedo, 2012)

15. De gevolgen van een digitale aanval die mijn bedrijfscomputer beschadigt zijn voor mijn bedrijf groot.
    - Sterk mee oneens
    - Oneens
    - Neutraal
    - Eens
    - Sterk mee eens

I believe protecting my organization's information is:
Likert scale 1/7 unimport -> important (Ifinedo, 2012)

16. Informatiebeveiliging binnen mijn bedrijf vind ik belangrijk**.**
    - Sterk mee oneens
    - Oneens
    - Neutraal
    - Eens
    - Sterk mee eens
    - Weet ik niet

I view information security attacks on my organization as:
Likert scale 1/7 harmless 1 harmful 7 (ifinedo, 2012)

17. De gevolgen van een cyberaanval op mijn organisatie zijn groot.
    - Sterk mee oneens
    - Oneens
    - Neutraal
    - Eens
    - Sterk mee eens

I believe that the productivity loss to recover the damages (e.g., data loss, malfunctioning computer) from being infected by malware is a serious problem. (Herath and Rao, 2009).

18. Het verlies in productiviteit bij het herstellen van de schade (bv. dataverlies, computer die slecht werkt) van een digitale virusinfectie is een groot probleem.
    - Sterk mee oneens
    - Oneens
    - Neutraal
    - Eens
    - Sterk mee eens

I believe that the data/information loss from being infected by malware is a serious problem (Herath and Rao, 2009).

19. Het verlies van data/informatie na een digitale aanval of virus is een serieus probleem.
    - Sterk mee oneens
    - Oneens

- Neutraal
- Eens
- Hoe Sterk mee eens

Perceived vulnerability (5 times) :

It is possible that I will fall victim to a phishing attack (Williams & Joinson, 2020)

20. Het is mogelijk dat mijn organisatie slachtoffer wordt van een cyberinbreuk.
- Sterk mee oneens
- Oneens
- Neutraal
- Eens
- Sterk mee eens

The likelihood of an information security violation occurring at my workplace is (ifinedo, 2012):

21. Een inbreuk op de informatiebeveiliging binnen mijn organisatie is onwaarschijnlijk **(R).**
    - Sterk mee oneens
    - Oneens
    - Neutraal
    - Eens
    - Sterk mee eens

The likelihood of someone damaging my organization's computer systems is (ifinedo, 2012):

22. Een digitale inbreuk op mijn werkcomputer is waarschijnlijk.
    - Sterk mee oneens
    - Oneens
    - Neutraal
    - Eens
    - Sterk mee eens

My organization's information and data is vulnerable to security breaches (ifinedo, 2012):

23. De informatie en data binnen mijn organisatie is kwetsbaar voor cyberinbreuken.
    - Sterk mee oneens
    - Oneens
    - Neutraal
    - Eens
    - Sterk mee eens

I am at risk of falling victim to a phishing e-mail (Williams & Joinson, 2020)

24. Mijn organisatie loopt het risico slachtoffer te worden van cyberinbreuken
    - Sterk mee oneens
    - Oneens
    - Neutraal

- Eens
- Sterk mee eens

Coping Appraisal

Perceived response efficacy (3 times):

Enabling security measures at my workplace will prevent hackers from gaining access to important personal or financial information (Ifinendo, 2012) (disagree – agree)

25. Het implementeren van cybersecuritymaatregelen binnen mijn organisatie voorkomt dat hackers toegang krijgen tot belangrijke financiële- en persoonlijke gegevens.
    - Sterk mee oneens
    - Oneens
    - Neutraal
    - Eens
    - Sterk mee eens

At my work, efforts to ensure the safety of my confidential information are (Ifinendo, 2012) (Effective – ineffective)

26. Binnen mijn organisatie zijn maatregelen die informatiebeveiliging bevorderen effectief.
    - Sterk mee oneens
    - Oneens
    - Neutraal
    - Eens
    - Sterk mee eens

Performing any of the provided recommendations makes me feel safe when using my computer (Dang-Pham & Pittayachawan, 2015).

27. Het verbeteren van mijn online beveiliging geeft me een veilig gevoel.
    - Sterk mee oneens
    - Oneens
    - Neutraal
    - Eens
    - Sterk mee eens

Perceived Self-efficacy (3 times):

I have the expertise to implement preventative measures to stop people from getting my confidential information (Ifinendo, 2012) (Disagree – agree)

28. Ik heb de benodigde expertise om de voorzorgsmaatregelen te treffen die ervoor zorgen dat vertrouwelijke informatie binnen mijn organisatie beschermd is.
    - Sterk mee oneens
    - Oneens
    - Neutraal

- Eens
- Sterk mee een

I believe that it is within my control to protect myself from information security violations (Ifinendo, 2012) (Disagree – agree)

29. Ik geloof dat ik de beveiliging van systemen en informatie binnen mijn organisatie onder controle heb.
    - Sterk mee oneens
    - Oneens
    - Neutraal
    - Eens
    - Sterk mee eens

I feel confident when performing either of the provided recommendations (Lee et al. 2008)

30. Ik ben zelfverzekerd in het uitvoeren en verbeteren van de digitale veiligheid binnen mijn organisatie.
    - Sterk mee oneens
    - Oneens
    - Neutraal
    - Eens
    - Sterk mee eens

Response costs 3 times:

There are too many overhead costs associated with implementing IS security measures in my organization (Ifinendo, 2012)

31. Er komen te veel kosten kijken bij het implementeren van cybersecuritymaatregelen binnen mijn organisatie.
    - Sterk mee oneens
    - Oneens
    - Neutraal
    - Eens
    - Sterk mee eens

Enabling IS security measures in my organization is/would be time consuming (Ifinendo, 2012).

32. Het implementeren van cybersecuritymaatregelen binnen mijn organisatie kost te veel tijd.
    - Sterk mee oneens
    - Oneens
    - Neutraal
    - Eens
    - Sterk mee eens

The cost of implementing recommended IS security policy measures is: (Ifinendo, 2012) (lower than the benefits – exceeds the benefits).

33. De lasten zijn bij het implementeren van cybersecuritymaatregelen groter dan de baten.
    - Sterk mee oneens
    - Oneens
    - Neutraal
    - Eens
    - Sterk mee eens

7.2 Appendix B: Figures

Table 8
Collinearity Statistics

Variable	Tolerance	VIF
Perceived Severity	.746	1.31
Perceived Vulnerability	.789	1.27
Perceived Response Efficacy	.726	1.38
Perceived Self Efficacy	.759	1.32
Perceived Response Cost	.863	1.16

Table 9
Normal P-P plot

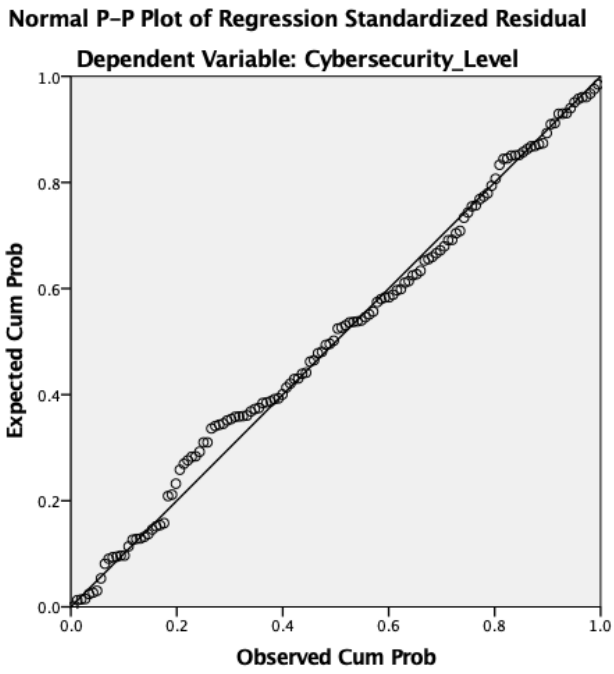

Table 10
Casewise Diagnostics

Variable	Std. Residual	Cybersecurity Level	Predicted Value	Residual
97	-3.253	18	30.5	-12.5

Table 11
Cook's Distance

	Minimum	Maximum	Mean	Std. Deviation
Cooks Distance	.000	.146	.008	.017

Table 12
Scatterplot

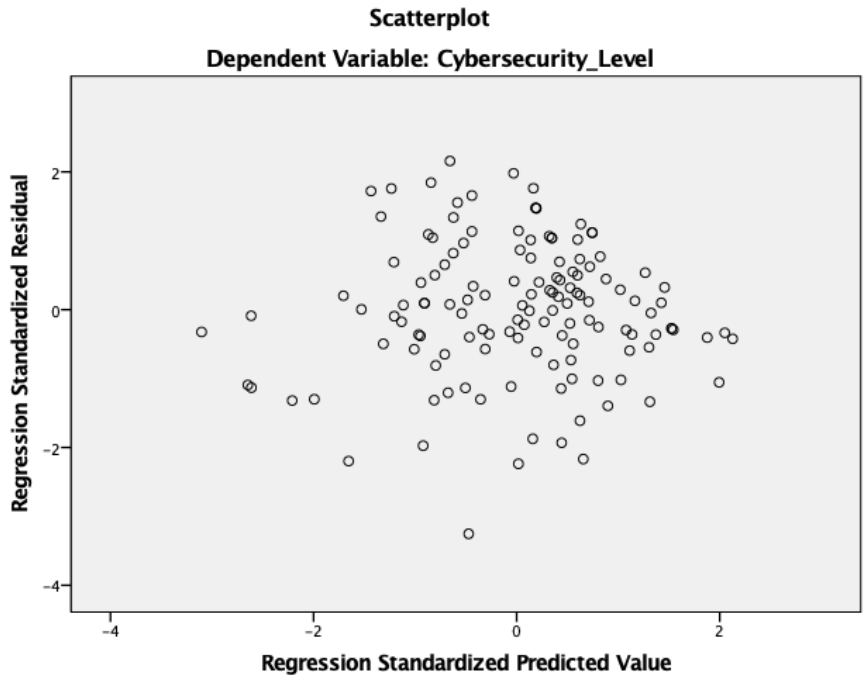

Table 13
ANOVA* results

Variable	Sum of Squares	Df	Mean Square	F	Sig,
Regression	2434.1	5	486.8	32.988	.000**
Residual	1889.1	128	14.8		
Total	4323.4	133			

*Dependent Variable: Cybersecurity Level
** Predictors: (Constant), Perceived Response Costs, Perceived Vulnerability, Perceived Self- Efficacy, Perceived Severity, Perceived Response Efficacy