RADBOUD UNIVERSITY

Nijmegen School of Management

Date: June 14th, 2022

Factors affecting the intention to adopt cyber incident response planning among Dutch SMEs: an empirical investigation

Master's thesis in Strategic management

Author: Falko Wielers (s4248864)

Supervisor: prof. dr. H.L. van Kranenburg (Hans)

Second reader: dr. K.F. van den Oever (Koen)

Abstract

To prepare for and, thereby, try to mitigate the negative impact of cyber incidents on SMEs, adoption of cyber incident response planning (CIRP) is imperative. This study aims to identify significant factors affecting CIRP adoption intention among Dutch SMEs. An integrated research model is developed based on the Technology-Organization-Environment framework, Diffusion of Innovation theory, Neo-Institutional Theory, and Protection Motivation Theory. The proposed model specifies one innovation (*relative advantage*), two organizational (*top management support, resource availability*), three environmental (*buyer/supplier pressure, external support, technological uncertainty*) and one decision maker (*cyber risk perception*) characteristic(-s) affecting CIRP adoption intention. The model is tested using survey data of 73 Dutch SMEs. Results of an ordinal logistic regression analysis show that top management support, buyer/supplier pressure, and cyber risk perception positively influence CIRP adoption intention. Overall, this study contributes to the cybersecurity adoption literature by demonstrating the usability of the theories in conceptualizing an integrated set of factors affecting CIRP adoption intention. Furthermore, a better understanding on what affects CIRP adoption intention is offered, which could help in making informed adoption decisions in at-risk SMEs and implementing policies or strategies aiming to promote CIRP adoption.

Keywords: Adoption intention, Cyber incident response planning, Cybercrime, Small and Medium-sized Enterprises, The Netherlands, Quantitative research

Preface

Completing this master thesis: '*Factors affecting the intention to adopt cyber incident response planning among Dutch SMEs: an empirical investigation'*, is my last step to graduate from Strategic Management. It is finally time to finish my time as a student at the Radboud University in Nijmegen. I would like to thank several people for helping me to conduct this master thesis. First, I would like to express my gratitude to supervisor prof. dr. H.L. van Kranenburg for the feedback he provided. I would also like to thank dr. K.F. van den Oever for being my second supervisor. Furthermore, all people who have helped to develop the questionnaire and gain an appropriate sample for the analysis are very appreciated. Fourth and finally, I would like to thank my girlfriend, family, and friends for their encouragement and provision of some interesting remarks.

Hopefully, this thesis will be an informative read.

Falko Wielers

Nijmegen, June 14th, 2022

List of abbreviations

Abbreviation	Description
APA	American Psychology Association
CBS	Central Bureau of Statistics *Dutch: Centraal Bureau voor de Statistiek*
CIRP	Cyber incident response planning
CIRT	Cyber incident response team
(D)DoS-attack	(Distributed) Denial of Service attack
DOI	Diffusion of Innovation Theory
DPA	Data Protection Authority *Dutch: Autoriteit Persoonsgegevens*
ENISA	European Network and Information Security Agency
ERP	Enterprise Resource Planning
EU	European Union
GDP	Gross domestic product
INT	(Neo-) Institutional Theory
IR	Incident response
IS	Information System
ISO	International Organization for Standardization
IT	Information Technology
KMO	Kaiser-Meyer-Olkin measure
Malware	Malicious software
NCTV	National Coordinator for Security and Counterterrorism *Dutch: Nationaal Coördinator Terrorismebestrijding en veiligheid*
NIST	National Institute of Standards and Technology
OLR	Ordinal Logistic Regression
PCA	Principal Component Analysis
PMT	Protection Motivation Theory
SANS Institute	SysAdmin, Audit, Network and Security Institute
SME	Small and Medium Enterprise
TOE	Technology-Organization-Environment framework
VIF	Variance Inflation Factor

Table of contents

1. Introduction

1.1 Problem statement

Cyber threats for organizations are permanent and growing (European Network and Information Security Agency [ENISA], 2021a; Central Bureau of Statistics [CBS], 2021; National Coordinator for Security and Counterterrorism [NCTV], 2020; Choo, 2011). While the accelerating digitalization offers economic and social opportunities for organizations, their growing reliance on information technology (IT) and data (Eurostat, 2022) makes them increasingly vulnerable to cyber incidents. For example, the Dutch Data Protection Authority (DPA) (2021), registered almost 23976 notifications of data breaches from Dutch organizations in 2020. Paoli, Visscher and Verstraete (2018) further state that cybercrime can cause negative effects on firms such as disruption of business continuity, loss of revenue, and recovery costs of IT-assets. Calculating the impact of cybercrime, cyber experts from Deloitte (2016) estimated that the expected value loss for the total Dutch economy is about 10 billion euros per year.

Despite large corporations and formal authorities typically making media headlines when it comes to cyber incidents, there is an increasing concern over cyber incidents for small and medium-sized enterprises (SMEs) (ENISA, 2021b). SMEs seem to be particularly vulnerable because they must deal with the same threat landscape as corporations but lack awareness of cyber threats and solutions, lack adequate resources to defend themselves, and underestimate their chances to become a victim (Bada & Nurse, 2019; Ponsard, Grandclaudon & Dallons, 2018; Saleem, Adebisi, Ande, & Hammoudeh, 2017; Osborn, 2015; Harsch, Idler & Thurner, 2014; Hayes & Bodhani, 2013). While definite victimization and impact figures of SMEs are lacking, it is estimated that SMEs are the victim of two out of three cyber-attacks (Fielder, Panaousis, Malacaria & Hankin, 2016), and the impact of cybercrime on SMEs is considered substantial (Aguilar, 2015). Thereby, SMEs are often seen as weakest link in supply chains, through which criminals gain access to corporations or authorities.

As SMEs may not always be able to avoid the negative impact of cyber incidents with prevention efforts (e.g., antivirus software, firewall), they could consider adopting a cyber incident response planning (CIRP) process. CIRP is a proactive approach to cyber incidents that aims to develop a formal (written) plan containing clear guidelines, roles, and responsibilities in handling cyber incidents. The National Institute of Standards and Technology (NIST), SysAdmin, Audit, Network and Security

(SANS) and International Organization for Standardization (ISO) all developed incident handling standards and frameworks (Ab Rahman & Choo, 2015) in which they recommend that a plan should address several components, such as the firms' critical IT-resources, cyber scenarios, the formation of a cyber incident response team (CIRT), external parties to be contacted, response flowcharts, and a communication plan. One important point to mention is that SMEs often will have different preparation schemes than larger corporations (Morreale, 2008). SMEs are expected to have limited IT-staff, who often do not have the necessary expertise and skills for the technical aspects in incident handling. Therefore, when facing a cyber incident, SMEs may need to call external experts to contain issues. However, this does not mean that SMEs do not need to plan. CIRP is relevant in this context as it could emphasize whether and when to contact external parties, what these parties are going to do and what actions the owner or employees should do themselves before, during and after cyber incidents.

The ENISA (2021b) suggests that adoption of CIRP is imperative for SMEs as it may help to mitigate the negative impact of cyber incidents. CIRP is assumed to help firms proactively address cyber incidents by reducing uncertainty and decision time for decision makers and, thereby, making their responses to cyber incidents more efficient and effective (NIST, 2018). Without CIRP, the response of SMEs to a cyber incident will be more likely ad hoc and unplanned (ENISA, 2021b). Such a reactive approach to cyber incidents could result in serious cyber harm like disclosure of confidential information, longer recovery times, longer disruption of business continuity, more lost revenue, loss of criminal evidence, decline of the firm reputation, legal and compliance issues with stakeholders, and negative psychological symptoms for employees and executives/owners.

Although the importance of CIRP adoption for SMEs is recognized, incident response preparation among SMEs is generally described as limited (Hoppe, Gatzert & Gruner, 2021). Responses of SMEs are expected to be ad hoc and reactive at the time incidents are detected (Ahmad, Hadjkiss & Ruighaver, 2012). Despite this statement, no scientific research is conducted on CIRP adoption (intention) and influencing factors among SMEs. From a broad perspective, it is found in general cybersecurity adoption literature that SMEs are slower in adopting cybersecurity practices/products than larger corporations or governments, creating a security divide (Heidt, Gerlach & Buxmann, 2019; Osborn, 2015). Previous scholars try to explain why slow SME cybersecurity adoption exist. For

example, Heidt, et al. (2019) point out that SME characteristics, such as the absence of skilled workforces and funds, inhibit cybersecurity investments. Others indicate the importance of executives' threat perceptions in fostering adoption, while building on Protection Motivation Theory (PMT) to predict SME adoption of anti-malware software (Lee & Larssen, 2009) or information security behaviour (Saban, Rau & Wood, 2021; Barlette, Gundolf & Jaouen, 2017). Furthermore, Kabanda, Tanner and Kent (2018) conducted a qualitative study on SME cybersecurity practices in developing countries and identified organizational (e.g., management support) and environmental (e.g., institutional pressures) factors. While these studies demonstrate a growing knowledge on cybersecurity adoption in SMEs, they also tend to focus on the adoption of security technologies while neglecting administrative innovations. As it is expected that CIRP adoption at SME level is still at a nascent stage, a study on CIRP adoption intention and its factors becomes relevant.

This study attempts to contribute towards the above-described knowledge gap using cybercrime, CIRP and adoption literature. By seeing CIRP as an administrative innovation, an integrated research framework explaining CIRP adoption intention among Dutch SMEs is proposed and tested. The framework is built on theoretical perspectives of the Technology-Organization-Environment (TOE) framework (Tornatzky & Fleischer, 1990), Diffusion of Innovation (DOI) theory (Rogers, 2003), Neo-Institutional Theory (INT) (DiMaggio & Powell, 1983), and PMT (Rogers, 1975). Combining these theories may help to find significant factors affecting CIRP adoption intention among SMEs. The TOE framework, DOI theory and INT are flexible frameworks that are often integrated at firm-level studies (Baker, 2011). The theories suggest that innovation, organizational, and environmental characteristics affect adoption. As previous authors have built on these theories studying similar planning or cybersecurity innovations (cf. Kim & Amran, 2018; Hsu, Lee & Straub, 2012; Skipper, Hanna & Cegielski, 2009; Bandyopadhyay & Schkade, 2004; 2000), they could provide a starting point for this study. Additionally, the PMT, as an individual-level behavioural theory, is added because this theory helps to identify how adoption of protective behaviours is determined by decision makers' threat appraisals. In SMEs, an owner/executive, or IT-employee typically has the ultimate responsibility for information security (Barlette, et al. 2017), while firm decision making is highly dependent on a sole or few individuals. Therefore, it is suggested that their threat appraisals are important in firm adoption.

1.2 Research aim and research question

Following the above problem statement, the aim of this explanatory research is:

> *Identifying which factors influence CIRP adoption intention among Dutch SMEs, to -promote the adoption of CIRP through the development of effective governmental policies and marketing strategies and -inform decision makers in at-risk SMEs.*

To reach this research aim, the following main research question needs to be answered:

> *Which factors influence CIRP adoption intention among Dutch SMEs?*

The following sub-questions need to be answered to give an answer to the main research question:

1. *What are different types of cybercrime that SMEs currently could face?*
2. *What are different types of impact that could result from a cyber incident at a SME?*
3. *What is CIRP –as a proactive way for SMEs to deal with cyber incidents?*
4. *What is CIRP adoption intention?*
5. *Which factors –as related to the innovation, organization, environment, and decision maker– could influence CIRP adoption intention?*

1.3 Societal relevance

According to the Dutch Central Bureau of Statistics (CBS) (2022), there are 423240 Dutch SMEs (2-249fte) in the second quarter of 2022, accounting for 20.3% of all firms in The Netherlands. Thereby, SMEs account for a large part of the respective total national employment. Given this important role for employment and job creation, along with SMEs share of the gross domestic product (GDP) and their contributions to innovation, SMEs are often seen as the 'backbone' of the (Dutch) economy (Leukfeldt, 2021; Verhees & Meulenberg, 2004). At the same time, as already described in the first paragraph of this chapter, it should be noted that cyber incidents could have a serious negative impact on SMEs and their stakeholders. Considering the important social and economic role of SMEs in The Netherlands, it would be important to mitigate the impact of cyber incidents on Dutch SMEs. From this perspective, the former study has societal relevance in two ways.

First, knowledge on business-related cyber threats, CIRP as a potential solution for actual occurrences of cyber incidents, and factors affecting CIRP adoption intention could assist (IT) decision makers in at-risk SMEs in learning about cyber threats and successful CIRP adoption processes. Knowledge about whether and why (other) Dutch SMEs prepare and plan for cyber incidents, could guide these decision makers in the adoption of systemic, effective planning and preparation strategies. This could help (IT) decision makers in making more informed CIRP adoption decisions for their firms, which ultimately could help to mitigate the negative impact of cyber incidents on their SME.

Second, the research findings of this study provide various external stakeholders of SMEs (such as government policymakers, industry associations, interest groups, cybersecurity firms, provider organizations of IT/cybersecurity products and services, consultancy firms, other larger firms with SME partners, and customers) with the needed knowledge for developing appropriate strategies and policies to enhance the diffusion and adoption of CIRP over SMEs in The Netherlands. Up-to-date insight into adoption intention of CIRP as well as critical factors of CIRP adoption intention is created. Such knowledge provides a better understanding of which factors actors should give (more) attention to in promoting the adoption of CIRP in Dutch SMEs. Consequently, awareness campaigns as well as the development of effective policies or marketing strategies could help to mitigate the problem of cybercrime on Dutch SMEs and, therefore, broader society.

1.4 Theoretical relevance

Research on adoption of cybersecurity innovations in SMEs remains scarce due to the newness of the cyber domain. This study adds to this lack of literature in two ways. First, this is the first study that combines the literature on cybercrime, CIRP and organizational innovation adoption while contributing to a better understanding of CIRP adoption at SMEs. Scholars have not yet sufficiently conducted studies concerning the relative new digitalization threats for SMEs. In general, it should be noted that research concerning planning and preparation in SMEs remains little (Herbane, 2010; Runyan, 2006). It is remarkable how little is known about the adoption of incident or crisis management in SMEs, especially considering the impact of incidents (or crises) for SMEs and the important social and economic roles they play in communities.

Second, this study expands the existing literature by conceptualizing and testing an integrated research framework which may help to better explain the adoption of CIRP among SMEs. This study can be seen as the first, preliminary effort in developing an integrated research framework that tries to explain CIRP adoption intention among SMEs. Building on theoretical foundations from the TOE framework (Tornatzky & Fleischer, 1990), DOI theory (Rogers, 2003), INT (DiMaggio & Powell, 1983) and the PMT (Rogers, 1975), several factors related to the innovation, organization, environment, and decision maker are proposed. The knowledge gathered by conceptualizing and empirically testing the factors from these four theories in the context of cybercrime could help determine the applicability of such theories for explaining CIRP adoption intention among SMEs. Subsequently, the study could help researchers in understanding and further developing research frameworks for adoption of CIRP or other similar innovations in SMEs.

1.5 Outline

The remainder of this study is organized in the following way. The second chapter starts with background literature on cybercrime, CIRP and innovation adoption. Description of different types of cyber threats and their impact on firms, the importance of CIRP for firms, CIRP as an innovation, and the four theories that could help with identifying potential factors explaining innovation adoption is provided first. Based on these theoretical foundations, an integrative research model explaining CIRP adoption intention among Dutch SMEs is proposed. In the subsequent methods chapter, the decisions for the quantitative research strategy, data collection, operationalization of the variables and data-analysis techniques are substantiated. Then, the results from the data-analysis are described in the fourth chapter. This includes the refinement and validation of the variables at interest, as well as the results from testing the proposed research model by using an ordinal logistic regression (OLR) analysis. The last chapter starts with interpretating the results of this study. Subsequently, the main research question is answered, the theoretical contributions of this study are discussed, the practical implications are identified, and the methodological limitations and recommendations for future research directions are addressed.

2. Literature review and research framework

This chapter consists of five paragraphs. The first four paragraphs provide the needed background literature as well as theoretical foundation for developing the research model. First, different cyber threats and the ways in which cyber incidents could harm firms are identified (§2.1), and CIRP as innovative tool to prepare for cyber incidents is proposed (§2.2). Then, it is described what is regarded CIRP adoption intention (§2.3). Subsequently, theories are described that are used as lenses to identify factors of the adoption of related innovations (§2.4). Finally, the theoretical underpinnings are utilized to propose a research model with factors explaining the CIRP adoption intention among SMEs (§2.5).

2.1 Business-related cybercrime: types and impact

The purpose of this paragraph is to give first indications derived from cybercrime literature about the potential cyber incidents that SMEs could face and may choose to prepare for. Therefore, a conceptualization of the potential cyber threats that SMEs currently face is given first. Here, several business-related cybercrimes are described. Then, it is discussed what negative consequences firms may endure when a potential cyber threat becomes a real cyber incident.

Cyberspace and types of business-related cybercrime

First, we look at what is regarded cybercrime in a business context. To understand business-related cybercrime, the overarching 'cyber(-space)' concept must be understood. In recent years, cyber is used to describe almost anything that deals with computers and networks (Ottis & Lorents, 2010). Cyber is used in new terms related to security such as cyber defence, cyber terrorism, cyber-attacks, and cybercrime. All these examples have something to do with cyberspace as the environment for the specific concept in question. According to Ottis and Lorents (2010) cyberspace is: "*a time-dependent set of interconnected information systems and the human users that interact with these systems"* (p.3). The interconnection between the set of systems and human users in the above definition emphasizes that changes in cyberspace can take place in a very short time span and may affect a huge number of users (and therefore organizations). For example, a cyber-attack on one system may spread out to other systems within minutes or seconds, affecting every user of the systems. Lezzi, Lazoj and Coralla (2018) further argue that cyberspace consists of infrastructures and information. The infrastructure is regarded the hardware, servers, facilities, or software, while the information is extracted from the data sources.

Now cyberspace is defined, it can be argued what constitutes the abuse of technology in a cyberspace environment. It is suggested that a cyber threat is: "*any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service*" (NIST, 2012, p.8). The actual materialization of a cyber threat is called a cyber incident. Note that this study only addresses cyber incidents that are intentional crimes, not accidental (e.g., employee failure), structural (e.g., system failure due to aging) or environmental cyber incidents (e.g., natural disaster).

While it is only logical to suggest that cybercrime is the materialization of a cyber threat, there exists no uniform definition of cybercrime in literature (Payne, 2019; Paoli et al., 2018; Holt & Bossler, 2016; 2014). The variety of approaches towards cybercrime, and their related problems, demonstrate the difficulty in defining the concept. Paoli et al. (2018) state that some authors identify specific techniques, such as malicious software (malware) and (Distributed) Denial-of-Service ((D)DoS) attacks, that constitute cybercrime. Such typologies disregard legal definitions and, as technology quickly changes over time, become quickly outdated. Another approach is focusing on specific outcomes regardless of the technology that is used (Paoli et al., 2018). For example, cybercrime is described as a data breach regardless of the technique used to commit the crime. However, this creates ambiguity as techniques used to cause the data breach may differ. Finally, authors develop a 'technology-neutral' approach by focusing on activities that are formally defined as offences.

Despite differences in cybercrime definitions, commonly, a distinction is made between cyber-enabled crimes and cyber-dependent crimes (Maimon & Louderback, 2019; De Cuyper & Weijters, 2016; Holt & Bossler, 2016; McGuire & Dowling, 2013; Wall, 2007). These categories differ in the role of IT. First, cyber-enabled crimes are all the offenses in which IT is used in a supporting capacity (modus operandi) of the crime. However, IT is not the target of the crime. These are traditional forms of crime now committed using IT. For example, fraud in which products are bought by organizations but not delivered by providers. Second, cyber-dependent crimes are activities that can only be performed using IT. Here, IT is both the instrument and the target. Such crimes cannot exist without computer technology. An example is a (D)DoS attack in which the access to IT systems is being denied.

Following the classification discussed above, Paoli et al. (2018) describe five mutually exclusive types of cybercrime that might target firms. The authors do not define cybercrime per se, but rather identify specific acts that constitute cybercrime. Thereby, their typology is technology-neutral and based on legal and policy documents as well as academic studies. The five different cybercrime types that might target business organizations are: *illegal access to IT-systems, cyber espionage, data/system interference, cyber extortion,* and *internet/financial fraud.* Most of the crimes in the first three cybercrime types belong to the cyber-dependent crimes, while most of the crimes in the last two cybercrime types refer to cyber-enabled crimes. For each classification of the cybercrime acts, several techniques can be used. For example, a cybercriminal could use phishing (technique) to gain illegal access to one's data (criminal act). Below the business-related cybercrime types as well as the commonly used techniques to commit that crime are described. *Table 1* provides an overview of the different types.

Illegal access to IT-systems

First, criminals try to gain access to IT-systems of business organizations (Paoli et al., 2018). IT-systems are: "*any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*" (Council of Europe, 2001 in: Paoli et al., 2018, p.402). Cybercriminals could attain illegal access using malware, Trojan horses, backdoors, password sniffers and vulnerability exploitation. In addition, cybercriminals also socially engineer log-in information through supporting (cyber-enabled) techniques such as phishing and pharming. Therein, an illegitimate party tries to convince someone to perform an action (e.g., visiting a website, sharing information, sending money) under the assumption that they are engaging with a legitimate party. Offline techniques such as checking documents from waste disposals are used as well. Finally, there is an insider threat in which legitimate insiders (e.g., unsatisfied employee) misuse their access privileges.

A related concept of illegal access to IT-systems is hacking. Hacking can be described as gaining unauthorized access to IT-systems with criminal intention (Grabosky, 2016). Accordingly, Wall (2001) sees cyber-trespassing as an act in which an invisible boundary of an online environment is illegally crossed. Often, hacking is considered as a starting point of other cybercrimes described below, as cybercriminals could hack to disrupt, destroy, or adjust the IT-systems and data of organizations.

Cyber espionage

A serious crime for which a cybercriminal needs to gain illegal access to IT-systems first is called cyber espionage (Paoli et al., 2018). Digital forms of espionage are becoming more relevant as the value of sensitive data and the ability to access this data is safer and less risky than other types of spying (Søilen, 2016). Crane (2005) argues that espionage can be seen as the access to sensitive information without obtaining approval by the holder of the information. When an espionage attempt is successful, it results in theft of confidential and protected information, while the criminal remains invisible for the victim. Several types of data can be spied upon such as bulk business data (e.g., customers and financial data), data on high-value intellection property (e.g., R&D output) and data containing tactical corporate information (e.g., contract and strategy documents). Cybercriminals can use different techniques to espionage such as spyware, which is a particular type of malware.

Interference of data and/or systems

Another type of cybercrime that could, but does not necessarily, follow hacking includes either interference of data or interference of systems (Paoli et al., 2018). Data interference is about intentionally damaging, deletion, deterioration, alternation, or suppression of data without right, while system interference is the hindering of the functioning of a computer system (European Council, 2001 in: Paoli et al., 2018). In practice, most of the data and system interferences are provoked by malware infections coming from outside the organization (Paoli et al., 2018). However, they could also be performed by individuals who first gained illegal access to the data or systems. Additionally, system interference can also be caused by (D)DoS-attacks or spamming. In such situations, the capacity of systems become overloaded due to a massive quantity of data (requests) sent to the system. This could eventually result in partly usable or even unusable IT systems.

Cyber extortion

Cyber extortion is the extortion of businesses by encrypting IT-systems and data (Paoli et al., 2018). The term is used when cybercriminals obtain unlawful advantages due to threats or violence. Cyber extortion is mostly committed by combining ransomware with extortion offences (Paoli et al., 2018). Ransomware is a type of malware that encrypts IT-systems and data. This makes the IT-systems and data unusable for its users. After the ransomware infection, the extortion starts. Criminals may ask

organizations ransom money for regaining access to their encrypted data or systems. Paying these bribes may give them access to their systems or data again. Cybercriminals could also attempt to extort hush money by threatening to publish stolen data or by asking prevention money for future attacks. In essence, ransomware falls within the cyber-dependent category as it can only be installed on computers, while extortion falls within the cyber-enabled crime as it can also be committed without the use of a computer.

Internet fraud

The fifth form of business-related cybercrime includes fraud committed through the Internet. Paoli et al. (2018) see three types of fraud that are most frequently affecting businesses, namely: banking fraud, advance fee fraud and consumer fraud. In banking fraud criminals obtain money by fraudulently posing as a bank. In advance fee fraud the victim is promised to receive a large sum of money in return for a small up-front payment. Once the victim pays, the criminal makes up some further payments or simply disappears. Consumer fraud is committed when services or products are purchased online but either are never delivered or are of lower quality than promised. This internet fraud category is regarded a cyber-enabled crime because these internet crimes can also be committed in more traditional manners. For example, banking fraud can be committed without the use of online technology.

Table 1 – Cyber threats for firms (Source: Paoli et al. 2018)

Illegal act	**Description**	**Examples of commonly used techniques**
Illegal access to IT-systems	Illegal access to the whole or a part of an IT-system.	Hacker tools (backdoors, spoofing, password sniffer, password guessing), malware (Trojan horse), social engineering (phishing, pharming, spoofing)
Cyber espionage	Illegal interception of computer data from an IT-system.	*Always uses techniques in illegal access to IT-systems* Malware (spyware), interception of -bulk business data, -high-value intellectual property data or -tactical corporate information
Interference of data and/or IT-systems	Illegal damaging, deleting, deteriorating, alternating, or suppressing of computer data and/or IT system.	*Could use techniques in illegal access to IT-systems* Malware (Trojan horse, virus, worm), (D)DoS attack, spamming
Cyber extortion	Illegal encrypting data and/or IT-system and subsequent exploitation by demanding money, goods, or behaviour.	*Could use techniques in illegal access to IT-systems* Malware (ransomware), extracting money to unblock systems or data, extracting hush money to avoid confidential data from disclosure, extracting protection money to avert or stop an attack
Financial / Internet fraud	Using the Internet for the purpose of scamming victims out of money, property, or inheritance.	*Could use techniques in illegal access to IT-systems* Advance fee fraud, consumer fraud, internet banking fraud

Impact of cybercrime on firms

Following the description of cybercrime, the potential ambiguous impact of the above-mentioned cybercrime types on firms and their (external) stakeholders is discussed. This is important because by describing the negative impact of cybercrime for firms and their (external) stakeholders, the need for proactive responses towards cybercrime that aim to mitigate the negative impact can be identified.

Previous scholars focused on the cyber harm concept to describe the impact of cybercrime (Paoli et al., 2018; Agrafiotis et al. 2018; Anderson et al., 2014). Agrafiotis et al. (2018) identified five types of cyber harm that can manifest itself as a direct or indirect result from a cyber incident: physical and/or digital harm, economic harm, psychological harm, reputational harm and social and/or societal harm. First, digital harm is damage, unavailability, or theft of digital assets such as the hardware, software, and data (Agrafiotis et al., 2018), while physical harm includes bodily injury of individuals. Second, economic harm can be seen as the negative financial or economic losses such as reduced cost and investments. Paoli et al. (2018) discussed economic harm as harm towards material support (e.g., cost regarding personnel and lost assets, hard- and software replacement) and operational integrity (e.g., interruption of internal operational activities, provision of services to customers). Third, psychological harm indicates a negative impact to mental well-being described in negative emotions such as anxiety, guilt, or fear (Agrafiotis et al., 2018). Fourth, reputational harm is about the general opinion held about an entity as businesses could look weak due to cyber-attacks (Paoli et al., 2018). Finally, social/ societal harm includes harm towards societal trust in technology. One point to mention here is that all harm types can be interpreted in economic terms. Therefore, economic harm may overlap with other types of harm. For example, a cyber incident affects the firms' reputation which causes economic harm. Additionally, it must be noted that not only the firm itself can be harmed but other dependent stakeholders as well.

In practice, one cyber-attack commonly involves different illegal acts, techniques, harm types and victims. For example, phishing lures an employee to a fraudulent website. Thereby, the illegal activity fraud is committed. Then, ransomware is installed on the firms' IT-systems after which extortion begins. The firm needs to pay bribes, otherwise the IT-systems and data will be destroyed. As cybercriminals could also try to gain access to the IT-systems of other dependent external stakeholders through the victimized firm as well, these dependent stakeholders can be attacked and harmed next.

2.2 Cyber incident response planning for SMEs

This paragraph introduces CIRP as a specific planning process that can be used by SMEs to prepare for cyber incidents and, thereby, aims to mitigate the impact of cyber incidents for the firm and stakeholders. Therefore, we first look at what is incident response (IR), after a further description of CIRP is given.

IR refers to: "*the collective actions taken to resolve or mitigate an incident, coordinate and disseminate information, and implement follow-up strategies to stop future similar incidents from occurring*" (Ab Rahman & Choo, 2015, p.46). Several guidelines with different steps in incident handling are developed for large firms but also for SMEs, including cybersecurity incident response frameworks from institutes such as the NIST (Cichonski et al., 2012), SANS (Kral, 2011; Morreale, 2008), and ENISA (Maj et al., 2010) (Ab Rahman & Choo, 2015 for an overview of IR frameworks; Benz & Chatterjee, 2020 for a SME cyber preparedness evaluation tool). For example, the NIST separates preparation, identification, containment, eradication, recovery, and lessons learned.

In the preparation phase, a plan is developed containing clear guidelines, policies, procedures, roles, and responsibilities. In this regard, CIRP is defined as: "*The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attack against an organization's information system(s)"* (Swanson, Bowen, Philips, Gallup and Lynes, 2010, p.G-2). In accordance with planning literature (Coombs, 2014; McConnell & Drennan, 2006; Elsubbaugh, Fildes & Rose, 2004; Preble 1997; Reilly, 1993), it is prescribed in the guides above that this process aims to develop a plan with components such as a list of at-risk IT-resources, identification of scenarios, CIRT formation, a list of internal and external parties to be contacted (e.g., strategic decision makers, external digital forensics, legal, and communication experts), response flow charts and communication plans. After the plan is developed, it is shared among employees and tested in practice.

One should note that having a CIRP does not always mean that SME owners, executives, or employees execute all IR actions by themselves during a cyber incident. As SMEs often lack employees with experience to investigate cyber incidents, external parties must be contracted where capabilities are lacking. Furthermore, the plan is not left with (outsourced) IT-staff but requires the attention of the whole firms. In accordance, Harsch et al. (2014) state that when IR is solely seen as a technically centric endeavour, it will have blind spots for other key stakeholders who should have insights into the situation.

2.3 Intention to adopt cyber incident response planning

Based on recent developments of cyber threats and introduction of CIRP, a need to gain better knowledge on CIRP use among SMEs has become apparent. Therefore, this study will investigate the intentions to adopt CIRP by treating it as an innovation, that is: "*an idea, practice, or object that is perceived as new by an individual or other unit of adoption*" (Rogers, 2003, p.12). More specifically, CIRP fits with the idea of an administrative innovation (cf. Hsu et al., 2012), as it encompasses the development of a preparative program, including development of policies, structures, and processes. CIRP is a continuous process related to management activities, affecting the firms' social system. Seeing CIRP as an innovative tool in management practices to battle cybercrime, unlocks the broadly developed innovation adoption literature to define CIRP adoption intention below.

To define what is regarded CIRP adoption intention in this study, it must first be discussed what is seen as adoption. Scholars suggest that adoption is a process involving different phases (cf. Damanpour & Schneider, 2006; Rogers, 2003; Frambach & Schillewaert, 2002). Although such models differ in phases, it is suggested that two main stages of initiation and implementation, are separated by an adoption decision. The initiation stage consists of activities in which information about innovations are accumulated and evaluated. Therein, it could be stated that decision makers become aware of an innovation, form attitudes and adoption intentions (Frambach & Schillewaert, 2002). Eventually, this leads to the decision to adopt or reject. Adoption can be defined as: "*a decision to make full use of an innovation as the best course of action available"* (Rogers, 2003, p.177), and rejection is the decision to not adopt. The final implementation stage describes the employment of the innovation in firms from initial use, continued use to routinization. This could include exercising plans or evaluating performances.

While definite CIRP adoption figures are lacking, it is expected that a small number of SMEs are current users of CIRP. Due to the potential early timing of this study in which it is expected that CIRP adoption is still in a nascent stage, it is chosen to focus solely on adoption intention and not on the adoption decision or further implementation. Following Rogers (2003) definition of the adoption decision, CIRP adoption intention is described as the willingness of a firm to decide whether to use CIRP. It signals the firm's intention to use the innovation before actual adoption behaviour.

2.4 Theories used in previous studies on adoption of related innovations

To support the development of a research model explaining CIRP adoption intention among SMEs, relevant theories are discussed next. First, the TOE-framework of Tornatzky and Fleischer (1990) is described as an overarching framework describing several types of characteristics influencing adoption in firms. Then, three other relevant theories are described, being the DOI theory from Rogers (2003), the INT from DiMaggio and Powell (1983) and the PMT from Rogers (1975). Before the theories are discussed, it must be mentioned that, to best of the researcher's knowledge, there are no studies performed that conceptualize and/or empirically test relationships between factors and CIRP adoption intention. Therefore, conceptual, and empirical studies that use the theories to explain the adoption of other, but related cybersecurity or planning innovations are discussed below.

Technology-Organization-Environment framework

The widely accepted TOE-framework of Tornatzky and Fleischer (1990), as originally presented in IT/IS adoption studies, provides a starting point for many adoption studies. The framework identifies three contexts of a firm that influence adoption, including the technological context (technology availability, technology characteristics), organizational context (formal and informal linking structures, communication processes, size, slack resources), and environmental context (industry characteristics and market structure, technology support infrastructure, government regulation). Baker (2011) states that researchers use different versions of the TOE-framework drawing on the three contexts but selecting different factors at interest as they suggest that innovations are adopted in different contexts.

Empirical support for factors from the TOE-framework is found in several studies on the adoption of IT/IS innovations, such as the adoption of Enterprise Resource Planning (ERP) systems (Awa, Ukoha, Emecheta & Liu, 2016), and many others. While the TOE-framework is primarily developed for technology adoption, the theory is sometimes also used to propose factors affecting the adoption of other types of innovation. A relevant, conceptual study comes from Kim and Amran (2018) that use the framework to propose factors leading to adoption of business continuity planning among businesses. As well, Hasan et al., (2021) used the TOE-framework to capture multiple theories underlying various technological, organizational, and environmental factors of firms' cybersecurity readiness. In a similar way, the TOE-framework is deemed a relevant starting point for this study.

Diffusion of Innovation theory

To provide a richer insight in potential adoption factors, the theoretical lens from the DOI theory of Rogers (2003) is often added to the TOE-framework. Rogers suggests three categories of factors that influence innovation adoption: innovation characteristics, organizational characteristics, and individual characteristics. First, it is suggested that five characteristics of the innovation persuade decision makers to adopt innovations (relative advantage, complexity, compatibility, trialability, observability). For organizational characteristics, a difference is made between internal characteristics (centralization, complexity, interconnectedness, slack, size) and external characteristics (system openness). Finally, the individual characteristics could influence that adoption of innovation as well (leader change attitude).

The DOI theory is broadly used in SME adoption literature focusing on IT/IS adoption (cf. Tan, Eze & Chong, 2009). Despite most scholarly efforts focusing on technology adoption, two relevant studies using the DOI theory while focusing on the adoption of planning-related innovations can be found. The first study of Skipper et al., (2009) found that several innovation characteristics affecting the adoption of contingency planning conducted to prepare for disasters in a supply chain. Secondly, Bandyopadhyay and Schkade (2004) used the DOI theory to explain disaster recovery planning among American hospitals to prepare for IT-disasters. Consequently, it is imposed that the DOI theory can be used to identify potential adoption intention factors related to CIRP as the innovation at interest.

(Neo-) Institutional Theory

In INT, it is proposed that innovation adoption is driven by a search for legitimacy (Abrahamson, 1991). Legitimacy is the perception that actions of an entity are desirable within some socially constructed system of norms, values, and beliefs (Suchman, 1995). To maintain legitimacy, and therefore guarantee survival for a period, firms in the same environment tend to adopt similarities. DiMaggio and Powell (1983) suggest that three institutional pressures exert influence on organizations to become isomorphic (similar): coercive, mimetic, and normative. Mimetic pressures impose that firms imitate behaviour from other firms that are perceived similar or successful. Coercive pressures are imposed through firms' stakeholders, such as expectations from customers/suppliers or regulatory requirements from governments. Normative pressures arise from what is considered appropriate, learned from formal education and professionalization.

INT has been successfully used to explain firm behaviours. In IS/IT adoption literature it has received growing acceptance (cf. Liang, Saraf & Hu, 2007; Teo, Wei & Benbasat, 2003). Relevant for this research are studies that have used the theory to address firm cybersecurity behaviours. For example, Hsu et al. (2012) used the INT to study institutional influences on information systems security innovations. Cavusoglu, Cavusoglu, Son and Benbasat (2015) investigated organizational investment in information security control resources. They found that organizations make varying level of investment in such security control resources due to institutional pressures. Furthermore, Jeyaraj and Zadeh (2020) researched institutional isomorphism in organizational cybersecurity using a text analytics approach. Following these studies, the INT provides further suggestions to include factors from the firm's external environment (external pressures) influencing CIRP adoption intention in SMEs.

Protection Motivation Theory

Finally, the PMT of Rogers (1975) is an individual-level expectance-valence theory that suggests that two cognitive appraisal processes determine a persons' protection motivation (adoption intention) and actual behaviour (adoption). First, threat appraisals are individuals' assessments of the severity and vulnerability of a threat driving protective motivation. Second, coping appraisals include individuals' assessments response-efficacy, self-efficacy, and response cost. Positive relationships are expected between the efficacy variables and protection motivation, and a negative relationship is expected between response cost and protection motivation. To form the appraisals, two types of information sources on threats and coping behaviours are used: intrapersonal (prior experience, personality) and environmental (communication, observational learning).

The PMT is extensively used to study individuals or households' responses to threats. Only recently, the theory has been proposed in the cybersecurity domain. Relevant for this study are scholars that examined the influence of owners/executives' appraisals in SME responses towards cyber threats, such as SME adoption of information security measures (Barlette, Gundolf & Jaouen, 2017) or anti-malware software (Lee & Larsen, 2009). These authors suggest that owner/executives' appraisals are important for organizational adoption because they are usually the main decision makers regarding security topics in SMEs. Building on this notion, the theory is added as a lens to study the influences of risk perceptions affecting CIRP adoption intention.

2.5 Formulating an integrative research model

By incorporating the above-mentioned theoretical lenses, an integrated research model predicting CIRP adoption intention can be proposed. The TOE framework, DOI theory, INT and PMT are used to identify four types of characteristics that could affect CIRP adoption intention. Seven factors at interest for this study are identified, including innovation characteristics (*perceived relative advantage*), organizational characteristics (*top management support*, *resource availability*), environmental characteristics (*buyer/supplier pressure*, *external support*, and *technological uncertainty*), and decision maker characteristics (*cyber risk perception*). The rationale for each hypothesis is described below. The final proposed research model is visually presented in *figure 1* at the end of this paragraph (p.30).

Innovation characteristics

Following the DOI theory (Rogers, 2003), this study proposes that CIRP characteristics are important in adoption. From the five innovation characteristics that Rogers identifies, one characteristic is considered in the context of CIRP adoption intention among SMEs: *perceived relative advantage.*

Perceived relative advantage

Relative advantage, or perceived benefits, refer to: "*the degree to which an innovation is perceived as better than the idea it supersedes*" (Rogers, 2003, p. 15). In general, it is argued that innovations with clear, unambiguous advantages in effectiveness or efficiency are more easily adopted (Greenhalgh, Robert, MacFarlane, Bate & Kyriakidou, 2004). Benefits are shown to be key drivers of adoption of contingency planning at firms for supply chain disruptions (Skipper et al., 2009). For this study, the relative advantage of CIRP can be illustrated by how an established planning process (and use of the resulting plan) mitigate major losses following cyber incidents. Without planning, cyber incidents can cause major impact on organizations and stakeholders, such as interruption of business continuity, lost revenues, customer dissatisfaction and reputational harm (*see §2.1 for harm-types*). Decision makers that think that CIRP could comprehend the magnitude of such potential losses will perceive higher advantages and are expected to be more willing to adopt. The hypothesis is:

> *H1. A positive relationship will exist between perceived relative advantage and CIRP adoption intention among SMEs.*

Organizational characteristics

Both the TOE framework (Tornatzky & Fleischer, 1990) and DOI theory (Rogers, 2003) suggest that organizational characteristics influence adoption. This research examines two potential factors that could influence CIRP adoption intention: *top management support* and *resource availability*.

Top management support

Top management support is defined as: "*the continual active and enthusiastic approval of senior executives for proposed innovation"* (Sultan & Chan, 2000 p.111). In general, scholars found that top management support positively influence adoption of innovations (Abed, 2020; Skipper et al., 2009). It is argued that top management support is essential to maintain the importance of change (Thong, 1999). As decision makers in SMEs are very likely in the top management, their support is vital (Ramdani, Kawalek, & Lorenzo, 2009). Support may take several forms such as providing an articulated vision, sending signals of significance to employees and prioritization by allocation of appropriate resources. In the cybersecurity domain, Kabanda et al. (2018) found that SME adoption of cybersecurity in developing countries remains little due to minimal top management support. Likewise, it is expected CIRP adoption intention is driven by such management support. The hypothesis is:

> *H2. A positive relationship will exist between top management support and CIRP adoption intention among SMEs.*

Resource availability

Another proposed determinant from the TOE framework (Tornatzky & Fleischer, 1990) and DOI theory (Rogers, 2003) is the availability of adequate resources. Organizational resources are required for innovation adoption, sometimes also described as the organizational readiness. Authors have demonstrated stimulating effects of adequate resources on IT/IS innovation adoption in SMEs (Maduku, Mpinganjira & Duh, 2016; Lian, Yen & Wang, 2014; Ifinedo, 2011; Chang, Hwang, Hung, Lin & Yen, 2007), suggesting that firms need financial funds, time, and qualified human resources for successful adoption. Similarly, in crisis management literature it is stated by Spillan and Hough (2003) that SMEs often lack resources hindering crisis planning. It must also be noted that authors also argue that when a disaster hits the organization, smaller organizations do not have abundant resources to react and are therefore particularly vulnerable for its impact (Herbane, 2015; Corey & Deitch, 2011). Following the

rationale discussed above, this study suggests that SMEs only adopt CIRP if they have the resources. Thus, it is likely that firms with adequate money, qualified personnel for developing a plan and time needed, are more intended to adopt CIRP. In contrast, SMEs that lack the necessary resources are less intended to adopt CIRP. Subsequently, the hypothesis is:

H3. A positive relationship will exist between resource availability and CIRP adoption intention among SMEs.

Environmental characteristics

Based on the TOE framework (Tornatzky & Fleischer, 1990) and INT (DiMaggio & Powell, 1983), it is expected that three factors from the external environment are influencing CIRP adoption intention among SMEs: *buyer/supplier pressure*, *external support*, and *technological uncertainty*. The first variable can be considered a coercive pressure in INT, while the other two variables are considered the support infrastructure and industry characteristics extracted from the TOE framework.

Buyer/Supplier pressure

INT suggests that firms respond to coercive pressures within their environments to maintain legitimacy (DiMaggio & Powell, 1983). Authors have stated that IT/IS adoption is imposed by stakeholders such as customers, suppliers, or other trading partners (Abed, 2020; Ghobakhloo & Ching, 2019; Oliveira & Martins, 2010; Premkumar & Roberts, 1999). Stakeholders may use strategies to pressure a firm for adoption of innovations, such as recommendation, promises and threats. Empirical evidence is found for a broad range of innovations. Ghobakhloo & Ching (2019) found that imposition from trading partners, customers and the society is a significant and positive predictor of the adoption of smart manufacturing-related information and digital technologies such as enterprise resource planning, artificial intelligence, and augmented/virtual reality. Furthermore, Ghobakhloo et al. (2011) found that adoption of e-commerce applications in SMEs is significantly imposed by satisfying the expectations of buyer, suppliers, business partners and the industry at large. For this study it is expected that when SMEs experience pressure from cybersecurity expectations from customers, suppliers, or business partners, they are more inclined to adopt CIRP. Thus, the hypothesis is:

H4. A positive relationship will exist between buyer/supplier pressure and CIRP adoption intention among SMEs.

External support

External support refers to the availability of support from outside parties for successfully implementing and using an innovation (Sophonthummapharn, 2009; Premkumar & Roberts, 1999). Authors suggest that organizations are more willing to adopt IT/IS innovations when there is appropriate support for them (Premkumar & Roberts, 1999). SMEs could lack internal experts which hinders innovation adoption (Thong, 1999). They may overcome this difficulty by seeking support from external organizations in using the innovation. For example, receiving external support from vendors is a substantial attribute for Big Data Analytics adoption (Maroufkhani et al., 2020). As SMEs do not have the sufficient skills, using the available platforms and training programs may increase their capabilities for adoption. Similarly, this study suggests that support for adoption of CIRP could influence its adoption. SMEs could have a limited number of internal experts available that could develop a plan for cybercrime events. Therefore, the more external support for developing a plan is perceived, the more motivated an SME may be to adopt CIRP. Several organizations could provide aid in CIRP at the focal firm. For example, outside support may come from cybersecurity or consultancy organizations, cyber insurance companies, or the firms' IT-supplier. Hence, the following hypothesis is formulated:

> *H5. A positive relationship will exist between external support and CIRP adoption intention among SMEs.*

Technological uncertainty

The environment of an organization can be seen as a system outside a firm influencing firm behaviour. Decision makers in firms accumulate and interpret information about the environment prior to organizations reactions (Daft & Weick, 1984). Thereby, they seek for an equilibrium in response to uncertainty in their environment by changing strategies, structures, and processes. Environmental uncertainty can be defined as: "*the degree to which future states of the world cannot be anticipated and accurately predicted"* (Pfeffer & Salancik, 1978, p.67). It is suggested that rapidly changing and complex environments creates uncertainty, which in turn encourages adoption of innovations (Damanpour & Gopalakrishan, 1998; Grover & Goslar, 1993). For this study, a potential important type of uncertainty in the external environment comes from technologies. Technological uncertainty refers to the instability, complexity, and unpredictability of a technology (Land, Engelsen & Brettel, 2012;

Bstieler, 2005). Rapid changing IS/IT in industries, as well as many new products arisen from breakthroughs and many developments could reflect technological uncertainty. In such a rapidly changing technological environment, the need for CIRP to protect critical data and IS/IT is more pressing than ever. It is expected that when more technological uncertainty is perceived, a higher intention to adopt CIRP adoption follows. The hypothesis is:

H6. A positive relationship will exist between perceived technological uncertainty and CIRP adoption intention among SMEs.

Decision maker characteristics

Finally, it is suggested that the characteristics of decision makers in SME could influence CIRP adoption intention at organizational level. This expectation is based on the DOI theory (Rogers, 2003) that proposes that individual characteristics are important for organizational adoption, as well as the PMT (Rogers, 1975) describing individuals' responses to threat appraisals (perceived vulnerability). For this study, the variable of *cyber risk perception* is considered in the context of CIRP adoption intention.

Cyber risk perception

Memon, Raghubir and Agarwal (2008) see risk as the perception of the subjective likelihood assessment that an unfavourable or negatively valanced event will occur over a specified time period. Psychological models of individual responses to threats, include risk perception as a predictor of protective behaviours (Rogers, 1975). Based on such models, studies previously examined the relationship between a range of natural disaster risks and adoption of disaster preparedness measures. For example, a positive and significant relationship was found between risk perception of business owners and the adoption of earthquake preparedness measures (Han & Nigg, 2011). Howe (2011) finds that hurricane preparedness of business owners was a positive predictor of the precautionary actions. This indicates that decision makers with higher risk perceptions are more likely to prepare for disasters. With relevance to this study, the decision makers' risk perception in the context of cybercrime (*see §2.1 for different types of cyber threats*) is examined. It is expected that when decision makers perceive that it is likely their firm will become a victim of a cyber incident, the firm is more willing to adopt CIRP. Thus, the hypothesis is:

H7. A positive relationship will exist between decision makers' cyber risk perception and CIRP adoption intention among SMEs.

Control variables

To ensure that the observed variances can be assigned to the identified variables, this study controls for *firm size* and *firm industry (information and communication industry)*. These two control variables are selected based on previous adoption studies. The selected variables that potentially control the above-described relationships are briefly discussed below.

Firm size is commonly defined (and measured) as the number of firms' employees (Carmeli & Schaubroeck, 2008; Shaeffer & Mano-Negrin, 2003). Despite few scholars having theoretical interest in firm size, it is commonly used as a stand-in variable of other variables. Rogers (2003) states that firm size is one of the best predictors of organizational innovativeness as it is a surrogate measure of several dimensions (e.g., culture, slack resources, structure) affecting adoption. Firm size has been conceptualized to positively influence innovation adoption (Hameed et al., 2012; Rogers, 2003; Frambach & Schillewaert, 2002). It is often argued that firm size has a positive relationship with adoption as larger organizations have more resources, skills, and abilities to survive failures. Also, in disaster preparedness literature, firm size is a consistent factors of disaster preparedness which predicts that adoption of preparedness measures towards natural disasters (Han & Nigg, 2011; Howe, 2011; Ritchie et al., 2011). The above implies that firm size could be an important control variable.

The second control variable of firm industry refers to the sector to which the organization primarily belongs. Jeyaraj and Zadeh (2020) suggest that cybersecurity responses may differ between organizations in sectors who deal more often with IT products and services and other industries. In this study it is particularly relevant to test whether organizations that operate in the Information and Communication industry are more intended to adopt CIRP.

Visual presentation of the proposed research model

The final research model is shown in *figure 1*. The dependent variable of the research model is CIRP adoption intention. Seven independent variables are suggested: *relative advantage, top management support, resource availability, buyer/supplier pressure, external support, technology uncertainty,* and *decision makers' risk perception*. To account for further variances in the dependent variable *firm size* and *firm industry* (*Information and Communication industry*) were also included in the model. Now the research model is constructed, the methods used to test the model can be discussed in the next chapter.

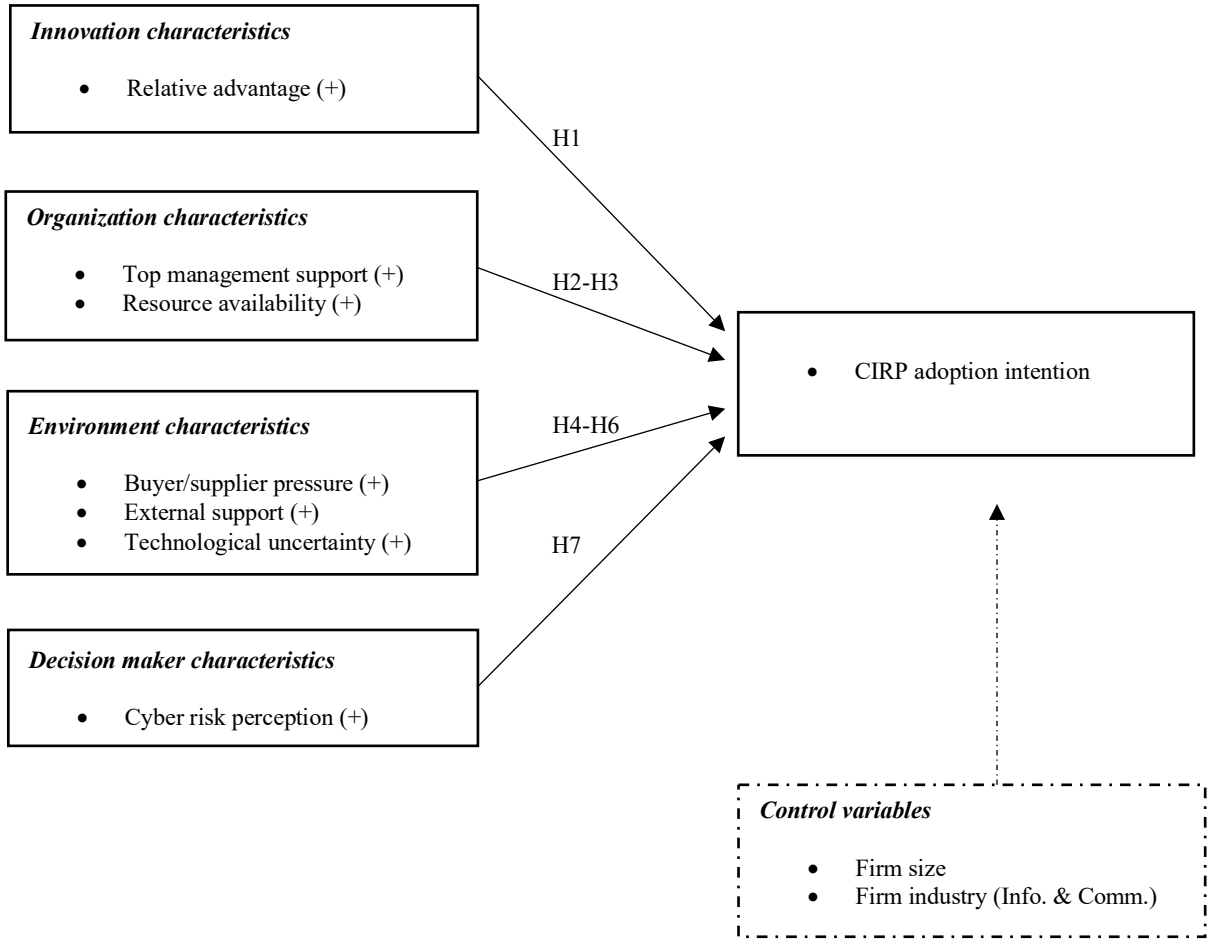


Figure 1 – Proposed research model explaining CIRP adoption intention among Dutch SMEs

3. Methods

In this chapter, the choices made for the used research methods are described and substantiated. In the first paragraph, the reasons to use a quantitative research strategy with online surveys are described (§3.1). Subsequently, the research context, data collection procedure and used data sources are examined (§3.2). Afterwards, the operationalization of the research variables (§3.3) and the rationale for the used analytical methods (§3.4) are discussed. Finally, a description of the followed guidelines to perform the study in an ethical way are given (§3.5).

3.1 Research strategy

The main research objective of this study is to explain CIRP adoption intention among SMEs. To reach this objective, an empirical (as it is based on primary data gathered from Dutch SMEs), explanatory (as cause-effect relationships were examined), deductive (as hypotheses were formulated based on adoption theories and then accepted/rejected based on practical evidence) and quantitative (as numerical data was collected using an online survey and analysed with statistical methods) research approach is adopted. Quantitative research is a mean for the deductive testing of relationships between variables (Creswell, 2014). From a postpositivist worldview, several hypotheses can be formulated and tested through the collection and analysis of numerical data. The online survey provides a numeric description of opinions of a large population towards a certain subject (Van Thiel, 2014). Prepared, close-ended questions are asked, and respondents can provide answers based on standardized response scales.

The chosen research approach best fits our research aim for several reasons. First, the theory-driven (deductive), quantitative research approach is appropriate to address the research problem as hypotheses about CIRP adoption can be formulated based on a large amount of general adoption theories and empirical studies on similar innovations. Furthermore, the online survey typically provides an efficient method for collecting a large amount of data from many SMEs. Scholars (cf. Creswell, 2014; Van Thiel, 2014; Field, 2013) indicate that the large scale and high standardization levels makes survey efficient ways of collecting data, helps protecting against subjectivity by gathering many responses, makes it able to test relations between variables and identify the strength of these relations, control for differing explanations, generalize results over a larger population and more easily replicate findings.

The research process of this study can be defined as an iterative process, which means that repeated steps were taken during the process. After a search for gaps in the relevant literature, the main research objective and approach are specified. Subsequently, a research model with hypothesis is formulated. Different steps were taken to test the research model including the development of the questionnaire, control of the content validity of the questionnaire, the collection of the data, control of the reliability and convergent and discriminant validity of the research variables and, finally, the examination of the proposed research hypotheses. To clarify the full research process, a reproduction is shown in *figure 2* below.

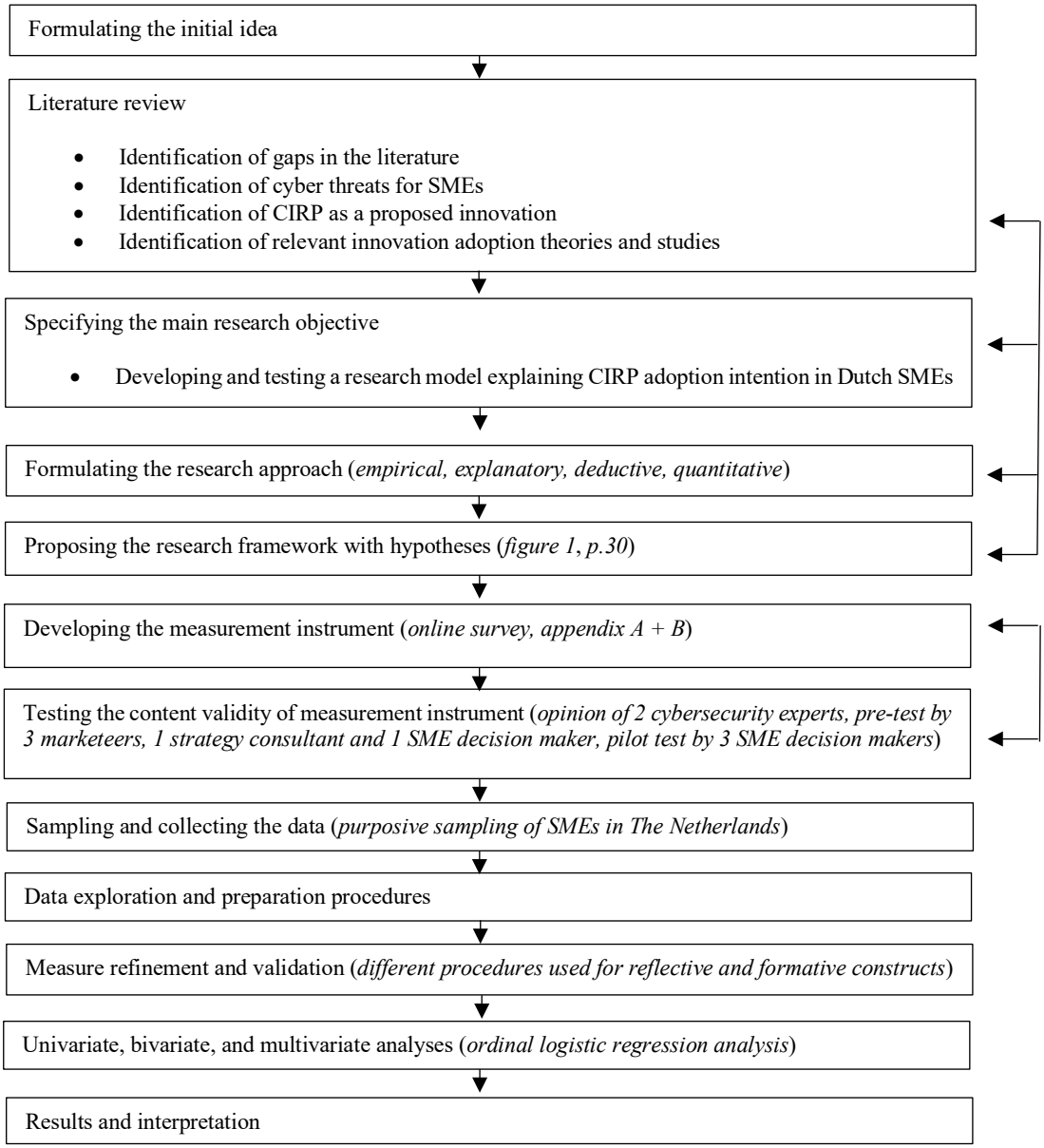


Figure 2 - Research process

3.2 Data collection and research sample

This paragraph describes from who, and how the data for this study is collected. First, the reasons for choosing the Dutch research context are described. This is followed by a description of the data collection procedures, the sampling method used and the profile of the final research sample.

Research context

The Netherlands was chosen as this study's research context as SMEs operating in The Netherlands seem to be easy, yet lucrative targets for cybercriminals. As noted in the introduction, Dutch SMEs serve as backbone the economy of The Netherlands. According to the Dutch government statistics (CBS, 2022), 20.3% of Dutch organizations are categorized as SME (2-249fte), providing a large part of the Dutch GDP. SMEs further account for Dutch employment and job creation. In general, it is suggested that Dutch firms are highly digitalized (DPA, 2021). Despite these factors making SMEs in The Netherlands potential attractive targets for cybercriminals, Dutch authorities and interest groups suggest that the needed defences in SMEs are lacking and promotion of cybersecurity initiatives is needed. For example, the Dutch Cyber Security Council (2021) argued that cybercrime resilience should have a top priority and MKB-Nederland, calls for new action programs concerning cybersecurity in SMEs.

Data collection

The study uses data collected from an online survey that was set up in Qualtrics software. The survey includes questions about the constructs formulated in the research model, demographics, and some additional information (*see §3.3 for the development of the measurement instrument*). The sampling frame of the online questionnaire are SMEs in The Netherlands that had not adopted CIRP. To fall within the category of SMEs, an organization needs to have less than 250 full-time equivalent and/or an annual turnover not exceeding 50 million and/or an annual balance sheet not exceeding 43 million (European Commission, 2015). However, based on remarks from initial test respondents it is assumed that respondents do not want to disclose annual turnover and annual balance sheet figures. Therefore, only the employee criterium is followed. As this study is focused on providing an understanding of the adoption of CIRP among SMEs in The Netherlands, it was chosen to include all SMEs from all different industries.

Within each SME, one decision maker involved in innovation adoption is approached to participate. In SMEs, top management directly affects CIRP adoption processes. The owner, chief information officer and CEO is often the same person who makes the adoption decisions. This is supported by the fact that top managers oversee their entire organizations' decision-making processes. Sometimes, IT managers/specialist make cybersecurity adoption decisions. Hence, top-level decision makers and IT-employees were targeted. The lack of access to a database with contact information from potential respondents made it necessary to use a non-probability purposive and convenience sampling methods for collecting data. Thus, the researcher made a purposive selection of the unit of analysis (Van Thiel, 2014). While this method has generalization implications, all available SMEs can be contacted.

Data was collected through email/telephone acquisition and personal connections. For acquisition, SMEs were initially contacted by telephone. Managers who agreed to participate in the study received an invitation to the online survey through e-mail. The invitation messages included requests for their participation in the study, a short description of the researcher, research purpose, research confidentiality as well as a link towards the questionnaire. Additionally, the personal connections of the researcher are contacted. Potential respondents in the researchers' personal network were approached through direct invitation messages by email, but other channels (LinkedIn, WhatsApp) are used as well. The researcher also tried to tab into the networks of influential SME experts (cybersecurity, crisis communication, marketing) and one SME owner. These personal contacts of the researcher agreed to send invitations to firms in their own personal network with potential respondents.

Research sample

During the end of December 2021 until February 2022, a total of 101 surveys were collected in Qualtrics. To address missing values and outliers, data cleaning processes were performed in IBM SPSS v.28. From the initial data exploration, it became clear that 20 cases did not finish the survey and had too much missing data. Furthermore, two cases showed remarkable responses, such as answering 'neutral' to every question and one additional outlier was found. Because these three responses have substantial influence on further analyses, they were deleted. Finally, responses from five SMEs were also removed as they are current CIRP users. The final dataset consists of 73 usable surveys for further analysis. Due to the way in which the data is collected, the response rate cannot be accurately calculated.

Table 2 – Sample characteristics; Individual level (n=73)

	Category	Adoption intention level						Total	
		No/Low (*n*=19)		Moderate (*n*=34)		High (*n*=20)			
		Freq.	%	Freq.	%	Freq.	%	Freq.	%
Gender	Male	16	84.2%	30	88.2%	18	90.0%	64	87.7%
	Female	3	15.8%	4	11.8%	2	10.0%	9	12.3%
Age	18-25 years	3	15.8%	1	2.9%	0	0.0%	4	5.3%
	26-35 years	5	26.3%	6	17.6%	2	10.0%	13	17.8%
	36-45 years	5	26.3%	13	38.2%	7	35.0%	25	34.2%
	46-55 years	2	10.5%	8	23.5%	6	30.0%	16	21.9%
	56-65 years	4	21.1%	5	14.7%	5	25.0%	14	19.2%
	Older than 65 years	0	0.0%	1	2.1%	0	0.0%	1	1.4%
Education level	Primary education	0	0.0%	0	0.0%	0	0.0%	0	0.0%
	Secondary education	2	10.5%	3	8.7%	0	0.0%	5	6.9%
	MBO	5	26.3%	4	11.8%	2	10.0%	11	15.1%
	HBO	7	36.8%	16	47.1%	12	60.0%	35	47.9%
	WO	5	26.3%	10	29.4%	6	30.0%	21	28.8%
	PhD	0	0.0%	1	2.9%	0	0.0%	1	1.4%
Position	Owner / CEO	15	78.9%	25	73.5%	15	75.0%	55	75.3%
	CFO / CTO / CCO / COO	2	10.5%	4	11.8%	1	5.0%	7	9.6%
	CIO / IT director / IT manager	0	0.0%	2	5.9%	0	0.0%	2	2.8%
	IT specialist	1	5.3%	2	5.9%	2	10.0%	5	6.8%
	Other managers	1	5.3%	1	2.9%	2	10.0%	4	5.5%
Job experience	Less than 1 year	0	0.0%	0	0.0%	1	5.0%	1	1.4%
	1-5 years	11	57.9%	7	20.6%	7	35.0%	25	34.2%
	6-10 years	3	15.8%	7	20.6%	3	15.0%	13	17.8%
	11-15 years	0	0.0%	6	17.6%	3	15.0%	9	12.3%
	16-20 years	3	15.8%	6	17.6%	4	20.0%	13	17.8%
	More than 20 years	2	10.5%	8	23.5%	2	10.0%	12	16.4%

To gain insights in the final research sample, the sample characteristics are described next. According to the characteristics at individual level (*table 2*), more men than women finished the survey. This emphasizes the idea that (IT) decision makers in SMEs are more often masculine. It can be claimed that the respondents have appropriate knowledge about their firms' decision-making as 55 respondents (75.3%) were the owner of the participating firm. From a firm level perspective (*table 3*), it can be concluded that the sample includes firms from a wide range of industries. Note that respondents from firms in the information and communications industry (*n*=14, 19.2%) as well as the advisory, research, and other business services (*n*=20, 27.4%) are overrepresented, indicating potential non-response bias. The sample further includes 30 micro enterprises (41.1%), 29 small enterprises (39.7%) and 14 medium enterprises (19.2%). The mean of firm size is 36.26fte. Additionally, 38 firms (52.1%) were more than 20 years old. On average, businesses were 27.45 years old. The dataset contains 62 firms that outsource (parts) of their IT-environment, suggesting a frequent dependency on IT-providers. Regarding CIRP adoption intention level it can be noted that 20 SMEs scored high (27.4%), 34 SMEs scored moderate (46.6%), and 19 SMEs scored low or no intention at all (26.0%).

Table 3 – Sample characteristics; Firm level (n=73)

	Category	Adoption intention level						Total	
		No/Low (*n*=19)		Moderate (n=34)		High (*n*=20)			
		Freq.	%	Freq.	%	Freq.	%	Freq.	%
Firm size	Micro (2-9 fte)	12	63.2%	13	38.2%	5	25.0%	30	41.1%
	Small (10-49 fte)	5	26.5%	14	41.2%	10	50.0%	29	39.7%
	Medium (50-249 fte)	2	10.5%	7	20.6%	5	25.0%	14	19.2%
Firm age	5 years or less	6	31.6%	2	5.9%	4	20.0%	12	16.4%
	6-10 years	2	10.5%	4	11.8%	3	15.0%	9	12.3%
	11-20 years	2	10.5%	8	23.5%	4	20.0%	14	19.2%
	More than 20 years	9	47.4%	20	58.8%	9	45.0%	38	52.1%
Firm industry	Agriculture, forestry, and fishing	1	5.3%	0	0.0%	0	0.0%	1	1.4%
	Manufacturing	2	10.5%	3	8.8%	1	5.0%	6	8.2%
	Construction	0	0.0%	1	2.9%	1	5.0%	2	2.7%
	Retail/wholesale	1	5.3%	6	17.6%	3	15.0%	10	13.7%
	Transportation and storage	0	0.0%	1	2.9%	0	0.0%	1	1.4%
	Hospitality	2	10.5%	0	2.1%	1	5.0%	3	4.1%
	Information and communication	3	15.8%	7	20.6%	4	20.0%	14	19.2%
	Financial services	0	0.0%	4	11.8%	1	5.0%	5	6.8%
	Real estate and trade	1	5.3%	0	0.0%	0	0.0%	1	1.4%
	Consultancy/business services	7	36.8%	7	20.6%	6	30.0%	20	27.4%
	Rental of movable property and other business services	1	5.3%	2	5.9%	2	10.0%	5	6.8%
	Culture, sport, and recreation	1	5.3%	1	2.9%	0	0.0%	2	2.7%
	Other	0	0.0%	2	5.9%	1	5.0%	3	4.1%
Market scope	Local	2	10.5%	1	2.9%	0	0.0%	3	4.1%
	Regional	8	42.1%	11	32.4%	8	40.0%	27	37.0%
	National	6	31.6%	16	47.1%	8	40.0%	30	41.1%
	International	3	15.8%	6	17.6%	4	20.0%	13	17.8%
IT outsourcing	Fully outsourced	4	21.1%	5	14.7%	2	10.0%	11	15.0%
	Partially outsourced	6	31.6%	15	44.1%	10	50.0%	31	42.5%
	Fully insourced	9	47.4%	14	41.2%	8	40.0%	31	42.5%

3.3 Operationalization

The measurement instrument is established through an extensive process of item selection and refinement. Primarily, it was tried to develop the instrument based on existing scales from prior literature. However, due to the uniqueness of CIRP in adoption literature some adjustment had to be made. For measures that are modified or proposed, guidelines were followed from the literature. As well, to describe IR, two meetings with two IR consultants were conducted. The draft survey was then examined and pre-tested by adoption experts (three marketeers, one SME digital transformation consultant, and one SME owner). Based on their critique, adjustments were made on length, wordings, and instructions. Before distributing the survey over a larger population, the survey was piloted at three SMEs to ensure understandability. Below, the variables are defined and, following criteria from Jarvis, MacKenzie and Podsakoff (2003), classified as either single-indicator, reflective, or formative construct. The final set of items that are included in the survey are shown in *Appendix A*. Furthermore, the routing of the survey is shown in *Appendix B*.

Dependent variable: Categorization of CIRP adoption intention groups

Adoption intention is described as the willingness of a firm to decide whether to use CIRP. CIRP adoption intention is considered an ordinal dependent variable, including three CIRP adoption groups (1=no/low, 2=moderate, 3=high). To classify each SME in one group, the survey followed the following process. First, a definition and explanation of CIRP is provided. Then respondents are asked whether they had heard of CIRP before the survey. Subsequently, respondents need to indicate whether their firm is a current user of CIRP, making it able to separate current adopter and non-adopter. Adopters are directed to questions about use of cyber training/exercises and excluded from further analysis. Non-adopters must indicate their intention to adopt CIRP at different timeframes (will never adopt CIRP, more than three years, two-three years, one-two year, within next year). These answer categories were then classified in three groups. First, no/low adoption intention includes all SMEs who never want to adopt or want to adopt within three years. Second, moderate adoption intention includes all SMEs who intend to adopt between one-three years. Third, high adoption intention includes all SMEs that want to adopt within one year.

Independent variables

All independent variables are discussed next. To adequately capture opinions of respondents, all the discussed independent variables are measured on 7-point Likert scales (1=strongly disagree, 7=strongly agree), except stated otherwise.

Innovation characteristics

One CIRP characteristics is measured: perceived relative advantage. Perceived relative advantage is defined as: "*the degree to which an innovation is perceived as better than the idea it supersedes*" (Rogers, 2003, p.15). This construct was assessed as a reflective construct focusing on the benefits of the innovation. Advantages related to response speed and effectiveness were identified based on conceptualizations of previous studies (Bandyopadhyay & Schkade, 2004; Premkumar & Roberts, 1999). As well, some further advantages specific to CIRP were proposed. The final measure included benefits such as the ability to lessen damage towards organizational reputation, shorten duration of business interruptions, lessen lost revenue, avoiding legal exposure, lessen recovery costs and lessen cost for (external) personnel that needs to handle cyber incidents.

Organizational characteristics

Two organizational characteristics are measured in this study: top management support and resource availability. Top management support is defined as: "*the continual active and enthusiastic approval of senior executives for proposed innovation"* (Sultan & Chan, 2000 p.111). Four items regarding top management support were retrieved from IT adoption studies (Lian et al., 2014; Premkumar & Roberts, 1999). These included items focused on whether managers see CIRP as strategically important for the firm and provide adequate resources. In accordance with the previous studies from which the items are derived, top management support is classified as a reflective construct. Second, resource availability refers to: *the extent to which resources are available in the organization to adopt a (technological) innovation"* (Maduku et al., 2016). Following Miller and Friesen (1982), all SME decision makers were asked whether their firm has the needed capital (money), skilled people and organizational time to adopt CIRP. Thereby, resource availability is regarded a formative measure in which money, skills and time form the construct.

Environmental characteristics

Three environmental characteristics are all measured as reflective constructs: buyer/supplier pressure, external support, and technological uncertainty. The first variable can be described as the amount of pressure experienced from buyers and suppliers to adopt an innovation. Four items were retrieved from previous studies on IT/IS adoption in SMEs (Ghobakhloo et al., 2011; Al-Qirim, 2007) and further modified for this study. Second, external support refers to the availability of support for implementing and using an innovation (Premkumar & Robers, 1999). Again, the items were retrieved from previous IT/IS adoption literature (Ghobakhloo et al., 2011; Premkumar & Roberts, 1999). Three items were modified to CIRP, measuring the level in which vendors (such as consultants, insurers) market, promote and provide support for CIRP. Finally, technological uncertainty is defined as: *"total amount and unpredictability of products or services technological changes in the industry."* (Terawatanavong, Whitwell, Widing & O'Cass 2011). Based on previous conceptualization of Bandyopadhyay and Schkade (2004), three measurement items measuring rapid changes in technology were modified for the purpose of this study. The included items were specifically focused on IT developments in the firms' industry.

Decision maker characteristics

Finally, one variable related to the specific characteristic of a decision maker is measured: cyber risk perception. Memon, Raghubir and Agarwal (2008) see risk as the perception of the subjective likelihood assessment that an unfavourable or negatively valanced event will occur over a specified time period. This description of risk guided the measurement of cyber risk perception in this study. The question concerning cyber risk perception began with a description of three common cyber scenarios that SMEs could encounter, as identified through the description of cyber threats (*see §2.1*). These are (1) CEO-fraud, (2) Ransomware and cyber extortion, and (3) (D)DoS-attack. Respectively, the three scenarios can be placed in categories of internet/financial fraud, cyber extortion, and interference of data and/or IT-systems from the business-related cybercrime conceptualization of Paoli et al. (2018). The likelihood of each scenario was then measured asking: How likely do you think that this cyber scenario occurs in your organization within the next five years? followed by a 11-point Likert-scale (1=extremely unlikely, 11=extremely likely). The 11-point Likert scale was used to provide respondents with many options of potential answers. Note that cyber risk perception is regarded a formative index in which perceptions of different risks form the construct.

Control variables

Two single-indicator control variables are included: firm size and firm industry. First, firm industry is described as the sector in which the organization primarily operates. Utilizing the categorization of standard business codes provided by the Dutch Chambers of Commerce, respondents had to indicate in which industry the firm was primarily operating. Based on the theoretical considerations, a dummy variable was created only for the information and communication industry (1=primarily active in the information and communications industry, 0=primarily active in any other industry). The second control variable 'firm size' is measured as the current number of full-time equivalents at the respondents' firm. Respondents were asked an open question regarding this number. Then, the responses were categorized as either micro enterprise (who have 1-9 full-time equivalent), small enterprise (who have 10-49 full-time equivalent), or medium enterprise (who have 50-249 full-time equivalent). Note that this is an ordinal variable as there is a logical order in the scale.

3.4 Analytical techniques

After the responses were collected, the data is downloaded from Qualtrics and imported in IBM SPSS V.28 to perform statistical analyses. The collected data is analysed using several quantitative analyses in a two-staged approach. Therein, a difference can be made between -measure refinement and validation and -univariate, bivariate and multivariate analyses of the constructed variables. The analytical techniques used in both phases are further described below.

Regarding the measure refinement and validation, different guidelines are followed to address the reflective scales and formative indexes. This is needed because the differences of reflective scales (observed variables are assumed to be caused by one latent variable) and formative indexes (observed variables are assumed to cause one latent variable) propose unique issues (Jarvis, MacKenzie & Podsakoff, 2003; Diamantopoulos & Winklhofer, 2001). For the reflective scales, steps as described by Field (2013) and Hair, Black, Babin and Anderson (2014) are taken. The reflective scales are estimated on construct validity and reliability. A principal component analysis (PCA) can be performed to understand the structure of the latent variables and reduce the data set to a more manageable size while retaining original information. PCA can be used to validate the structure of the research variables as identified and modified from previous studies. Then, reliability assessments are performed to estimate whether the measurers consistently reflect the construct. After handling the reflective scales, guidelines from Diamantopoulos and Winklhofer (2001) are used to handle formative indexes. Thereby, content and indicator specification as well as multicollinearity issues are addressed to construct an index.

The obtained reflective scales and formative index were further used for the univariate, bivariate and multivariate analyses. For the multivariate analysis an ordinal logistic regression (OLR) is used (also known as a cumulative logit model). OLR is an appropriate technique when a research problem involves one ordinal dependent variable with more than two categories, presumed to be related to two or more nominal, ordinal, or continuous independent variables (Osborne, 2015). In contrast to a multinomial logistic regression model, the OLR model can exploit the natural order of the ordinal dependent variable and, thereby, provides a more informative and powerful analysis. In the OLR model, the cumulative odds of events are expressed as a particular score or less. Thus, the cumulative odds for the levels of the dependent variable in this study are modelled as:

$\theta_1 = P$ (level 1) / P (level greater than 1)

$\theta_2 = P$ (level 1 or 2) / P (level greater than 2)

In these equations, θ is the cumulative odds ratio and P is the probability of a particular event. The equation of the third and last level of the dependent variable is not shown since the probability of scoring level 1, 2 or 3 is always equal to 1. These equations can also be expressed as follows:

$\theta_j = P$ (level $\leq j$) / (1 - P (level $\leq j$))

Where j is any category of the dependent variable (j=1,2,3). The cumulative logit can then be obtained by applying the natural logarithm transformation to the cumulative odd ratios:

Logit (θ_j) = Log (θ_j) for j = 1,2,3

Consequently, the coefficients of an OLR model reveal the extent to which the logit varies based on the values of the independent variables. Thus, in case of k independent variables, the general form of the OLR equation used for all the models in this study would be:

Logit (θ_j) = Log (P (level $\leq j$) / (1 - P (level $\leq j$))) = β_{0j} - ($\beta_1 x_1 + \beta_2 x_2 + \ldots + \beta_k x_k$)

Where j ranges from the number of categories of the dependent variable minus 1, β_{0j} is the intercept for the j category, $x_{1\text{-}k}$ are the independent variables affecting the logit and $\beta_{1\text{-}k}$ are the regression coefficients. The OLR analysis estimates j minus 1 (3-1=2 for this study) equations simultaneously. Therein, the model identifies a different intercept but a set of identical coefficients for each equation.

3.5 Research ethics

The sensitivity and secrecy of cybercrime issues and use of preparation measures makes research ethics particularly important for this study. To perform the study in an ethical way several procedural measures are taken following the guidelines and principles of the American Psychological Association (APA) (2017). Prior to the questions concerning the research variables, respondents are informed about what is studied, why the study is conducted, and how the study will be used. Subsequently, respondents could voluntarily decide whether they want to participate or not. To expose firms and participants towards the least amount of risk, full privacy is ensured. Concerning data management, it is promised that only the researcher and his supervisor(-s) would gain access to the collected data. This data is not used for any purpose other than this study. Access towards publishing the study in university databases is approved and only the participating firms are sent a copy of the study.

4. Results

The aim of this chapter is to present the results derived from the conducted analytical procedures. To ensure that the measurement of the proposed constructs was accurate, the measure refinement and validation of the reflective and formative constructs is described first (§4.1). After this assessment, the univariate and bivariate analyses are elaborated to gain insights in the used constructs (§4.2). Finally, the results of the OLR analysis are discussed (§4.3).

4.1 Measure refinement and validation

This study uses reflective, formative, and single indicator constructs. Reflective measurement, in which the observed variables (items) are assumed to being caused by a latent variable, is used for *perceived relative advantage, top management support, buyer/supplier pressure, external support*, and *technological uncertainty*. *Resource availability* and *cyber risk perception* are measured as formative constructs, in which items are assumed to cause latent variables. As the construction and assessments of reliability and validity are different for these different types of constructs (Diamontopoulos & Winklhofer, 2001), different procedures were used for refining and validating. The following sub-sections give insights in the results from these assessments.

Reflective constructs

The reflective constructs in this study were tested for validity and reliability to ensure that their measurement was accurate. Three types of construct validity can be addressed: content validity, convergent validity, and discriminant validity (Hair et al., 2014). Content validity concerns the level in which the items belonging to one construct cover its complete domain. Since the items of this study were based on previous literature and discussed with adoption specialists, it can be argued that the content of the constructs is valid. Subsequently, convergent validity is the degree to which items measuring one construct are correlated together to form that construct, while discriminant validity is the degree in which concepts differ from each other (Hair et al., 2014). To evaluate these last two types of validity, a PCA is conducted. Then, the internal consistency among each multi-item scale is assessed by executing reliability analyses. Finally, summated scales are constructed as a mean to overcome some measurement error in one construct, to represent multiple aspects of a concept in one measure and to make replication of the constructs across studies more easily. The two analyses are discussed below.

- **Principal component analysis**

A PCA is conducted to verify a simple component structure among the set of items. The main purpose of a PCA is to summarize the data, achieved by defining a smaller number of components that adequately represent the original set of items (Hair et al., 2014). The technique tries to explain the maximum amount of total variance in the correlation among items by transforming the original items into higher-order linear components (Field, 2013). Therefore, it looks for items that correlate highly with a group of other items, but do not correlate with items outside that group. The items that group together can be transformed into latent variables that can be used for further analysis. Below the assumptions for PCA are checked first, after which principal components were identified.

Checking assumptions before conducting the initial PCA

Before conducting the initial PCA, it should be checked whether PCA is an appropriate technique for the dataset used in this study. According to Field (2013), three statistical assumptions should be checked first: (1) the distribution of the data, (2) sampling adequacy and (3) collinearity among the included items of each component. Below, these three assumptions are checked.

The first assumption of normality is met since the included items are measured on Likert scales and the initial data exploration processes show that the included items roughly have normal distributions. Secondly, the sampling adequacy assumption is met as well. The sample size of the study is bigger than 50 observations and, therefore, acceptable for further PCA. Preferably, the sample size should have a 5:1 cases-to-variable ratio (Hair et al., 2014). While it was tried to obtain the highest cases-per-variable, the study must be based on this sample size due to difficulties in collecting large amounts of data. As well, the Kaiser-Meyer-Olkin (KMO) measure for multiple items verified the sampling adequacy of this study, KMO = .767 ('middling' according to Hutcheson & Sofroniou, 1999), and the KMO measures for individual items are above the acceptable limit of .50 (Field, 2013) (*see Appendix C, section 1)*. Finally, the third assumption is met, indicating some correlation among items but not too much. In the correlation matrix it is shown that sufficient strength of correlation among the items is found (at least .3 but not exceeding .9) (*see Appendix C, section 2*). Furthermore, a significant Bartlett's test of sphericity χ^2 (190) = 1033.906 $p < .001$ indicates that the correlations among the items significantly differ from zero. As all the assumption are met, an initial PCA can be conducted next.

Initial PCA

The first step of the initial PCA is to decide how many components a researcher should keep, also known as extraction (Field, 2013). The decision to keep components is based on the Kaiser criterion. Kaiser (1960) recommends that components with an eigenvalue greater than 1 should be extracted. Eigenvalues describe the amount of variance explained by one component, where an eigenvalue of 1 represents a substantial amount of variance (Field, 2013). An initial analysis is run to obtain eigenvalues for each component in the dataset using all the 20 items of the reflective constructs. A total of five components had eigenvalues greater than 1, explaining 74.551% of the variance (*see Appendix C, Section 3*). This leads to the conclusion to retain five components for further analysis.

With five components to be analyzed, the next step is choosing a rotation method. Rotation is used to gain a simple component structure and to make it easier to interpret the item loading patterns (Field, 2013). A distinction can be made between orthogonal rotation (uncorrelated constructs) and oblique rotation (correlated constructs). Some authors suggest that oblique rotation should be used because it is quite rare that a researcher measures a set of uncorrelated constructs, while others state that orthogonal rotation must be used due to its highly interpretable results. Hair et al. (2014) state that there are no specific rules on selecting a rotational technique. To choose between the two rotation methods, one should look at the needs of the research problem. As this study assumes that the theoretically important underlying constructs are uncorrelated, independence between components is assumed and orthogonal rotation (VARIMAX) is most appropriate.

By looking at item loadings in the initial rotated component matrix, representing bivariate correlations between the items and the components, decisions to eliminate items are made. Thereby, discriminant and convergent validity can be enhanced by respecifying the component matrix. Hair et al. (2014) state that standardized loading estimates should be .50 or higher, and ideally .70 or higher, to converge on a common construct. Furthermore, to assess discriminant validity, researchers can look for factor loadings that load on different components and have an absolute difference between loadings smaller than .20. With the initial rotated component matrix as a starting point, items must be chronologically eliminated. First, the lowest item loading should be eliminated, followed by the second lowest loading item, and so on. Then, cross-loaders can be identified and eliminated.

The initial rotated component matrix of this study showed no small component loaders (*see Appendix C, Section 4-5*). However, *ADV2* cross-loaded on two different components: perceived advantages and top management support. The item is about the time it takes before the firm can continue business operations as normal. To maintain a simple structure, it is chosen to eliminate the cross-loading item. Subsequently, it should be mentioned that the relative advantage construct does no longer include time-related advantages. Finally, it can be concluded that the final included items load uniformly on the intended components, and no further items needed to be eliminated based on the PCA.

After conducting the reliability analyses of each construct that was identified through the initial PCA above, it became clear that two additional items had to be eliminated: *PRE1* and *TEC3* (*further description at reliability analysis below*). While these items were not identified as low loaders or cross-loaders through the PCA, it was still decided to eliminate these items to increase the internal consistency of the constructs. The first eliminated item measures the pressure from the firms' industry to adopt CIRP (*PRE1*), which is not consistent with pressures from customers, suppliers, and business partners. The second item concerns the changing capabilities in organizations due to changing technological changes (*TEC3*), not consistent with the other uncertainty items. After elimination, 17 item were retained in the final unidimensional PCA solution. Insight in the final solution is given next.

Final PCA

The orthogonal rotated (VARIMAX) component matrix from the final PCA conducted on the remaining 17 items is shown in *table 4.* By checking the assumptions, it can be noted that PCA is suitable for this dataset. The KMO-measure verified sampling adequacy, KMO=.748 ('Middling according to Hutcheson & Sofroniou, 1999). Furthermore, all individual KMO values were above the threshold of .5 (*see Appendix C*, *section 6*), and a significant Bartlett's test of sphericity $\chi 2\ (136) = 864.452$, $p < .001$ is found. As already identified while testing the assumptions before conducting the initial PCA, the correlation matrix shows sufficient strength of correlation among the items. Five components with eigenvalues greater than 1, explained 78.130% of the total variance (*see Appendix C, section 7*). Also, the communalities of the items after extraction are above the threshold of .50 (Hair et al., 2014), describing significant levels of explanation of common variance. Hence, the solution demonstrates good convergent and discriminant validity of the constructs.

Table 4 –Final PCA: rotated component matrix (after scale purification)

Item	Component					Communality
	1	2	3	4	5	
ADV1	***.789***	-.158	.089	.205	-.047	.700
ADV3	***.740***	.189	-.046	.117	.039	.601
ADV4	***.791***	-.025	.213	.098	-.028	.681
ADV5	***.743***	.131	.081	.027	.085	.584
ADV6	***.716***	.277	.166	-.009	.225	.667
TOP1	.090	***.849***	.124	.095	.006	.753
TOP2	.300	***.787***	.131	.201	.104	.777
TOP3	-.136	***.755***	.216	.227	.040	.688
TOP4	.154	***.761***	-.011	.152	.314	.724
PRE2	.141	.167	***.903***	.155	.058	.891
PRE3	.095	.110	***.898***	.204	.146	.890
PRE4	.190	.130	***.889***	.225	.132	.911
SUP1	.071	.207	.316	***.850***	.092	.879
SUP2	.154	.195	.140	***.900***	.069	.896
SUP3	.200	.232	.194	***.826***	.237	.870
TEC1	.071	.223	.112	.170	***.880***	.871
TEC2	.068	.060	.161	.114	***.922***	.898
						Total
Eigenvalues -Rotated	3.143	2.889	2.776	2.564	1.911	13.283
% of variance	18.491	16.992	16.328	15.081	11.239	78.130

Note(s): ADV (relative advantage), TOP (top management support), PRE (buyer/supplier pressure), SUP (external support), TEC (technological uncertainty). Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization. Rotation converged in 5 iterations.

To make sure that the final rotated component matrix is justified, an oblique (DIRECT OBLIMIN) rotation method is applied and compared to the final solution using the orthogonal (VARIMAX) rotation method. Hair et al. (2014) state that researchers should always assess the comparability of an oblique method to the orthogonal results. While these different rotation methods usually show the same results, it should be identified whether this is true in this analysis. By examining the item loadings of each component in the pattern matrix after oblique rotation (*see Appendix C, section 8*), it was noted that the interpretation of constructs is the same as found with orthogonal rotation.

- **Reliability analysis**

To assess whether the items of each reflective construct that is identified during the PCA consistently reflect the construct that its measuring, the Cronbach's α was calculated for each of the five multi-item scales. One point to mention here is that the internal consistency cannot be calculated for single-indicator constructs (at least two indicators are needed to assess how closely related items are as a group) and formative constructs (maximizing internal consistency of a formative construct is unimportant because indicators are examining unique facets of a construct) (Petter, Straub & Rai, 2007). Therefore, the internal consistency for such constructs is not calculated, as shown in *table 5*.

From the reliability analyses of each construct that was identified through the results of the initial PCA, it became clear that items from two constructs needed to be deleted to increase its Cronbach's α: buyer/supplier pressure (*PRE1*) and technological uncertainty (*TEC3*) (*see Appendix D*). As already discussed, these items were already eliminated before calculating the final rotated component matrix (*table 4*). After elimination of the two items, all scales have Cronbach's α value of at least .834, exceeding the threshold of .700 recommended by the literature (Nunnally, 1978). Thus, the set of items are consistently measuring the constructs. Finally, summated scales are made for each identified reflective construct by averaging all its items.

Table 5 -Results reliability analyses (after elimination of ADV2, PRE1, and TEC3)

Construct	Number of items	Cronbach's α	Measurement
1. CIRP adoption intention	1	Not applicable	Single indicator
2. Perceived relative advantage	5	.834	Reflective
3. Top management support	4	.851	Reflective
4. Resource availability	3	Not usable	Formative
5. Buyer/supplier pressure	3	.943	Reflective
6. External support	3	.927	Reflective
7. Technological uncertainty	2	.883	Reflective
8. Cyber risk perception	3	Not usable	Formative
9. Firm size (Micro, small, medium)	3	Not applicable	Single indicator for each category
10. Firm industry (Info. & Comm.)	1	Not applicable	Single indicator

Formative constructs

Next to the five reflective scales validated above, two formative indexes are constructed for *resour*ce *availability* and *cyber risk perception*. As discussed before, these formative constructs are latent variables that are assumed to be caused by observed variables (Podsakoff, Shen & Podsakoff, 2006; Jarvis et al., 2003). Authors propose that a different guideline should be followed by researchers that aim to validate the index of a formative construct (Diamantopoulos & Siguaw, 2006; Diamontopoulos & Winklhofer, 2001). Thereby, several notions should be taken into consideration, including (1) content and (2) indicator specifications, as well as (3) multicollinearity among items of the scale.[1] Below, a description is given on the index construction.

To address whether the constructs and their indicators are specified accordingly, researchers should base their conceptualizations on extensive literature review (Diamontopoulos & Winklhofer, 2001). Regarding the formative constructs, the content and indicators were specified based on a literature review, and thereby it is claimed to be appropriate for this study. Still, cyber risk perception must be discussed. For this construct, three types of business-related cyber scenarios were explained, after which respondents were asked to assess the likelihood that their firm will experience each specific scenario within 5 years. Due to the length and duration of explaining more scenarios, only three scenarios were measured in the survey. However, from the conceptualization of business-related cybercrime of Paoli et al. (2018), it can be concluded the content and indicator validity of cyber risk perception can be enhanced by adding several unique cyber scenarios. Thus, take into consideration that the construct only describes decision makers perceptions of likelihood regarding these three scenarios.

Diamontopoulos and Winklhofer (2001) also state that multicollinearity among indicators of a formative construct forms an issue for its validity as such a construct is based on a multiple regression. Excessive multicollinearity among indicators makes it difficult to separate the distinct influence of one indicator on one construct. For the indicators of a reflective construct this is not an issue because only single regressions are involved from the latent construct (independent variable) to one indicator

[1] Diamontopoulos and Winklhofer (2001) propose a fourth notion to address validity of a formative construct (p.273). A 'MIMIC' model should be constructed using formative indicators of one latent variable as causes of reflective indicators from the same latent variable. Thereby, the researcher can assess the significance and contribution of individual indicators. Subsequently, irrelevant indicators can be eliminated from the index that were not found relevant. However, because this study does not use reflective measures for these concepts this prescribed action cannot be executed.

(dependent variable). To address this issue, the variance inflation factor (VIF) and Tolerance-values were calculated, as shown in *table 6*. The VIF indicates whether an independent variable has a strong linear relationship with all other independent variables (Field, 2013). A threshold of VIF higher than 10 is often taken as an indication that multicollinearity is problematic. The tolerance statistic is the reciprocal of the VIF, where a tolerance-value below .10 shows problematic multicollinearity and .20 indicates a potential problem (Field, 2013). The highest VIF-values are 1.513 (skilled people) and 1.489 (financial resources). As these values do not exceed the threshold, no indications of serious problems were found. Hence, all the items of the formative construct were retained. Finally, a resource availability index and a cyber risk perception index is constructed by averaging the items for each construct.

Table 6 - Multicollinearity among indicators of each formative construct

Item	Description	VIF	Tolerance
Resource availability			
Res1	Financial resources (money)	1.489	.672
Res2	Skilled people	1.513	.661
Res3	Organizational time	1.263	.792
Cyber risk perception			
Ris1	CEO-fraud	1.246	.802
Ris2	Ransomware and cyber extortion	1.104	.906
Ris3	(D)DoS-attack	1.203	.831

Note(s): The VIF-values and Tolerances were measured separately for each formative construct (e.g., indicator 1 (*Res1*) of formative construct 1 (*Resource availability*), relative to both indicator 2 (*Res2*) and indicator 3 (*Res3*))

4.2 Univariate and bivariate analysis

To get an impression of the above-developed constructs, the univariate and bivariate statistics are shown in *table 7* (p. 51). Additionally, *Appendix E* can be consulted for further univariate statistics providing background information on decision makers' awareness of cyber threats (*see Appendix E, section 1*), decision makers' utilization of several cyber threat information sources (*see Appendix E, section 2*), decision makers' likelihood assessments of experiencing each specific cyber scenario at their firm (*see Appendix E, section 3*) and firms' cyber experience (*see Appendix E, section 4*).

Univariate statistics

The univariate statistics of the research variables are described at the lower part of *table 7*. For good interpretation of the univariate statistics, readers need to remind that all the independent variables are measured on 7-point Likert scales except for cyber risk perception that is measured on a 11-point Likert scale. The dependent variable, CIRP adoption intention, consists of 3 categories. Finally, firm size is an ordinal measure including micro, small and medium enterprise categories, and firm industry (information and communication) is a dummy variable.

Among the 73 usable responses, there are 20 SMEs (27.4%) with a high intention to adopt CIRP, 34 SMEs (46.6%) with a moderate intention to adopt CIRP, and 19 SMEs (26.0%) with a low intention to adopt CIRP or are not intended to adopt CIRP at all. Therefore, first indications are found that SME decision makers are distributed regarding their decisions to adopt CIRP. For the independent variables, it can be emphasized that on average decision makers perceived CIRP as very advantages, indicating the mean of 4.98 at relative advantage. Vice versa, buyer/supplier pressure is, on average, perceived as very low, indicating the mean of 2.76 with a standard deviation of 1.36. SME decision makers further think that it is moderately likely that their firm will experience cyber scenarios, as shown by the mean of 5.40 of decision makers' cyber risk perception.

Bivariate statistics

A Pearson correlation-matrix with the bivariate correlations among the variables is shown at the upper part of *table 7*. Field (2013) indicates that there should be no substantial correlations above .90, and ideally not above .70, between the independent variables of a study to conduct a regression analysis. In the correlation matrix it is shown that there are no exceptionally high bivariate correlations between the independent variables. The three highest scores among the independent/control variables exist between resource availability and top management support reflected by r=.491, p <.01, external support and buyer/supplier pressure reflected by r=.483, p <.01, and external support and top management support reflected by r=.461, p <.01. Overall, it can be stated that the results show acceptable correlations among the independent variables. Now the univariate and bivariate statistics are discussed, we can proceed with the multivariate analysis.

Table 7 – Descriptive statistics and Pearson correlation matrix (n=73)

	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.[a]
1. CIRP adoption intention	**1.000**									
2. Perceived relative advantage	.312**	**1.000**								
3. Top management support	.528**	.263*	**1.000**							
4. Resource availability	.295*	.028	.491**	**1.000**						
5. Buyer/supplier pressure	.365**	.315**	.338**	.262*	**1.000**					
6. External support	.231*	.313**	.461**	.314**	.483**	**1.000**				
7. Technological uncertainty	.126	.193	.343**	.381**	.309**	.343**	**1.000**			
8. Cyber risk perception	.375**	.201	.092	-.054	.147	.004	.066	**1.000**		
9. Firm size	.257*	.209	.230*	.134	.266*	.303**	.210	.169	**1.000**	
10. Firm industry (Info. & Comm.) [a]	.038	-.119	.218	.251*	.017	.059	.343**	-.350**	.050	**1.000**
MEAN	2.01	4.98	4.34	4.19	2.76	3.25	3.75	5.40	1.78	.19
SD	.74	0.96	1.18	1.16	1.36	1.29	1.54	1.76	.75	.40
MIN	1.00	1.60	1.00	1.67	1.00	1.00	1.00	1.33	1.00	0.00
MAX	3.00	7.00	6.75	6.33	6.00	6.00	7.00	9.33	3.00	1.00
RANGE	2.00	5.40	5.75	4.67	5.00	5.00	6.00	9.67	2.00	1.00
SKEWNESS	-.022	-.551	-.430	-.287	.568	-.079	.277	-.181	.386	1.599
KURTOSIS	-1.122	.982	.243	-.649	-.571	-.812	-.999	-.295	-1.117	.571

Note(s):

[a] *Dummy variable* (1 = Information and Communication industry, 0 = all other industries)

* Significant at .05 level (two-tailed)
** Significant at .01 level (two-tailed)

4.3 Multivariate analysis

The obtained constructs are used in the subsequent OLR analysis. In this paragraph, several assumptions to conduct the analysis are checked first. Then, the fit of the model is assessed by providing the relevant summary statistics. Finally, the proposed hypotheses are tested to identify the significant effects between the independent variables and CIRP adoption intention.

Sample size requirements and further assumptions for OLR analysis

Hair et al. (2014) state that there is a general lack of assumptions in logistic regression analyses. In contrast to linear regression analysis or discriminant analysis, an OLR analysis does not assume normality, linearity between the independent and dependent variables, and homoscedasticity. Still, the analysis must meet an appropriate large sample size as well as the following four assumptions: the presence of a dependent variable on an ordinal scale, the presence of one or more independent variables on continuous, ordinal, or nominal scale, the absence of multicollinearity, and presence of proportional odds (Osborne, 2015; Hair et al., 2014; Field, 2013). Below, the assumptions are checked.

First, it should be noted that this study does violate appropriate sample size requirements. Hosmer and Lemeshow (2000) recommend total sample sizes greater than 400 for logistic regression analyses. Hair et al. (2014) further state that the sample size per category of the dependent variable should be at least 10 observations per independent variable. Because there are 9 independent variables in the full model, at least 90 observations are needed per category. However, due to difficulties in collection data from a large amount of decision makers (*see §5.5 for further discussion on this research limitation*), only 73 usable responses are collected. This small sample could have so much sampling error that identification of all, but the largest effects is improbable. Due to the practical difficulties in collecting a large amount of data it is still chosen to work with the small sample. In this regard, this study must be seen as a preliminary effort to be confirmed in further studies.

This study further meets the first and second assumption of the OLR analysis, by including one ordinal dependent variable and several dependent variables considered as ordinal or continuous variables (including dummies). The dependent variable of this study 'CIRP adoption intention' is measured on a ranked categorical scale, ranging from no/low adoption intention to high adoption intention. As well, there are nine predictor variables included that were measured on Likert-scales or

included as dummy variable. Note that variables measured on Likert-scales are essentially ordinally scaled but often considered as continuous variable. These properties of the study's variables make the OLR analysis an appropriate data-analysis technique to use in this study.

In addition, no problematic multicollinearity issues are found among the independent variables, fulfilling the third assumption. Multicollinearity exists when independent variables are highly correlated (Hair et al., 2014). Violating this assumption leads to untrustworthy results regarding the individual importance of independent variables (Field, 2013). To test for multicollinearity, two techniques are used. First, the Pearson correlation matrix is scanned to assess correlations among two independent variables. As discussed before, no substantial correlations above .90, and ideally not above .70, between the independent variables should exist. The Pearson correlation matrix (*table 7,* p.51) shows that no bivariate correlation value among the independent variables is problematic. Second, the VIF and tolerance values are calculated to address more subtle forms of multicollinearity. To identify these measures, a multiple regression analysis is conducted. In this multiple regression analysis, CIRP adoption was considered as a continuous dependent variable. As previously discussed, the Tolerance-value should not below 0.1 and VIF should be no larger than 10 (Field, 2013). Results in *table 8* (p.54) demonstrate that the tolerance values and VIF for all the variables do not exceed the thresholds.

Finally, the assumption of proportional odds is met. In an OLS model, different intercepts are created for each level of the dependent variable. For example, an intercept is created for the logit of adoption intention level 1 versus level 2 and level 3, and an intercept is created for the logit of adoption intention level 1 and level 2 versus level 3. Proportional odds entails that the coefficient of each independent variable has the same effect on the odds of the dependent variable, regardless of the intercept (Osborne, 2015). The assumption of proportional odds can be tested in SPSS with the test of parallel lines. In this test the obtained ordinal model containing one set of coefficients for all intercepts is compared to a model with separate sets of coefficients for each intercept. Because the test of parallel lines is found to be insignificant for model 1 ($\chi^2 = .245$ (df = 3), $p = .970$) and model 2 ($\chi^2 = 5.416$ (df = 10), $p = .862$) (*see Appendix F, section 1-2*), it can be argued that the coefficients of the independent variables are consistent for the different intercepts. In this regard, one set of coefficients can be used to describe the effects of the independent variables on CIRP adoption intention.

Table 8 - Multicollinearity among independent variables

	VIF	Tolerance
Independent variables		
Relative advantage	1.270	.787
Top management support	1.679	.596
Resource availability	1.489	.671
Buyer/supplier pressure	1.447	.691
External support	1.656	.604
Tech. uncertainty	1.483	.674
Cyber risk perception	1.297	.771
Control variables		
Firm size	1.176	.850
Firm industry (Info. & Comm.)	1.455	.687

Note(s): Dependent variable: CIRP adoption intention considered as continuous variable

Model fit

After assumption testing, two OLR models are run to test the direct effects of the seven independent variables and the two control variables on CIRP adoption intention. Because the order of variable entry could affect significance and effects of the dependent variables, a block-wise selection method is used. The first model adds only the control variables to the model: firm size and firm industry (Information and Communication industry). In the second model all seven independent variables are added to the equation. At the lower part of *Table 9* on the next page the summary statistics of the two models are provided. As well, *Appendix F section 1-2* provides the full SPSS output of the OLR analyses for both models. Below, the overall fit of the two models is discussed.

The -2Log likelihood statistic provides insights into how much unexplained variability there is in the data (Field, 2013). To determine whether the proposed model improves the ability to predict CIRP adoption, a chi-square test is performed to test the difference between the -2Log likelihood of the baseline model and the final model. For model 1, there is a non-significant (χ^2= 6.050 (*df*=3), *p*=0.109) difference in -2Log likelihood between the baseline model (34.940) and the final model (28.890). While for model 2 there is a significant (χ^2= 43.840 (*df*=10), *p* <.001) difference between the baseline model (154.897) and the final model (111.057). This means the proposed model 2 with dependent variables and control variables better fits the data than the original baseline models and, thereby, improve the ability to predict CIRP adoption intention.

Table 9 - Results of the OLR analysis (n = 73)

	Model 1 (Only control variables)							Model 2 (Independent variables + control variables)						
						95% confidence interval							95% confidence interval	
	Estimate	**SE**	**Wald**	**df**	**Sig.**	**Lower bound**	**Upper bound**	**Estimate**	**SE**	**Wald**	**df**	**Sig.**	**Lower bound**	**Upper bound**
Intercepts														
[CIRP adoption = 1]	-.434	.369	1.386	1	.239	-1.156	.288	7.285	1.974	13.615	1	<.001	3.415	11.154
[CIRP adoption = 2]	1.728	.428	16.277	1	<.001	.889	2.568	10.589	2.235	22.445	1	<.001	6.209	14.970
Dependent variables														
Relative advantage								.420	.298	1.985	1	.159	-.164	1.004
Top management support								.978	.310	9.946	1	.002	.370	1.586
Resource availability								.207	.268	.596	1	.440	-.318	.731
Buyer / Supplier pressure								.391	.228	2.948	1	.086	-.055	.837
External support								-.194	.250	.602	1	.438	-.685	.296
Technological uncertainty								-.279	.203	1.884	1	.170	-.677	.119
Cyber risk perception								.506	.174	8.458	1	.004	.165	.846
Control variables														
Firm size: Micro [a]	0[a]	.	.	0	.	.	.	0[a]	.	.	0	.	.	.
Firm size: Small	1.085	.507	4.574	1	.032	.091	2.079	.326	.586	.311	1	.577	-.821	1.474
Firm size: Medium	1.184	.626	3.578	1	.059	-.043	2.411	.563	.731	.595	1	.441	-.869	1.996
Firm industry: Not Info & Comm. [a]	0[a]	.	.	0	.	.	.	0[a]	.	.	0	.	.	.
Firm industry: Info. & Comm.	.086	.562	.023	1	.878	-1.015	1.187	.741	.757	.958	1	.328	-.743	2.225

	Value	**df**	**Sig.**	**Value**	**df**	**Sig.**
Model summary						
Nagelkerke's pseudo R^2	.090			.513		
-2Log likelihood	34.940			154.897		
-2Log likelihood (χ^2 test)	6.050	3	.109	43.840	10	<.001
Pearson statistic (χ^2 test)	.953	7	.996	139.416	134	.357
Deviance statistic (χ^2 test)	1.380	7	.986	111.057	134	.926

Note(s): Ordinal dependent variable = CIRP adoption intention *(*1 =no/low, 2 = moderate, 3 = high*)* [a] Reference category: SPSS sets parameter to 0 because it is redundant. [CIRP adoption = 1] includes the intercept of the logit of being in group 1 against the odds of being in group 2 or higher. [CIRP adoption = 2] includes the intercept of the logit of being in group 2 or below against the odds of being in group 3.

Second, goodness-of-fit measures are provided at the Pearson and Deviance statistics. For model 1, both the Pearson (χ^2 = .953 (*df* = 7), *p* = .996) and Deviance (χ^2 = 1.380 (*df* = 7), *p* = .986) tests were insignificant, resulting in a good fit of the model. As well, for model 2 the Pearson statistic (χ^2 = 139.416 (*df* = 134), *p* < .357) and the Deviance statistic (χ^2 = 111.057 (*df* = 134), *p* = .926) are clearly non-significant, showing indications of a good model fit. Note that there are large amounts of empty cells (e.g., dependent variable levels by observed combinations of predictor variable values) with zero frequencies that could affect these tests (Field, 2013). For example, model 2 shows 156 (66.7%) cells with zero frequencies. As there is little data to estimate the model, the goodness-of-fit statistics are still included but should be interpretated with caution.

Finally, the pseudo R^2 measures provide insights into the explanatory value of the proposed model (Field, 2013). Several pseudo R^2 measures are provided in *Appendix F*. Nagelkerke's R^2 is provided here due to its interpretability. Model 1 shows a Nagelkerke's R^2 of .090, explaining 9.0% of the variance in the dependent variable. Model 2 shows a Nagelkerke's R^2 of .513, indicating that the model explains 51.3% of the variance in the dependent variable. Thereby, the value of adding the independent variables in predicting CIRP adoption intention is identified.

Hypotheses testing

Now the summary statistics are discussed, the intercepts of the cumulative logits and the contribution of each independent variable can be described next. The results of the OLR analysis in the upper part of *table 9* should be interpretated in the following way. First, an intercept is created. These intercepts represent the border (in terms of a logit) where SMEs are predicted into higher categories. Note that the odds of being in CIRP adoption intention level 1 (=no/low adoption intention) is the complement of being in CIRP adoption intention level 2 or higher (=moderate adoption intention, high adoption intention), and being in CIRP adoption level 2 or below (=moderate adoption intention, no/low adoption intention) is the complement of being CIRP adoption level 3 (=high adoption intention). Subsequently, coefficients of the independent variables show how much one variable adds to reach the threshold. Take into consideration that the model assumes that each independent variable exerts the same effect on each cumulative logit, as previously confirmed at the test of proportional odds. The results of hypotheses testing are further discussed below, while *table 10* provides a summary of the tested hypotheses.

From the results in *table 9* it can be concluded that hypotheses regarding three independent variables (top management support, buyer/supplier pressure, cyber risk perception) are supported. First, it is found that top management support is highly significantly, and positively affecting the adoption of CIRP (b =.978, p = .002). Thus, *hypothesis 2 is supported at p <.01*. The results further show a significant influence of buyer/supplier pressure on CIRP adoption intention (b = .391, p = .086). This leads to the conclusion that *hypothesis 4 is supported at p <.10*. Finally, a significant result is found at decision makers' cyber risk perception affecting CIRP adoption intention (b = .506, p = .004). This result leads to the conclusion that *hypothesis 7 is supported at p <.01*.

The other four hypotheses are all rejected based on the results of the OLR analysis. Contrary to the expectations, a non-significant relationship of perceived relative advantage, resource availability, external support, and technological uncertainty on CIRP adoption intention is found. Therefore, *hypotheses 1, 3, 5, and 6 are rejected*. Regarding the control variables it is found that whether a SME belongs to the 'Information and Communication industry' exhibits no direct effect on CIRP adoption level. Furthermore, the firm size has also no significant influence on adoption intention among the sampled SMEs in the second model.

Table 8 – Summary of hypotheses testing

	Description	**Result**
H1	A positive relationship exists between relative advantage and CIRP adoption intention among SMEs.	*Rejected*
H2	A positive relationship exists between top management sup. and CIRP adoption intention among SMEs.	*Accepted (at p <.01)*
H3	A positive relationship exists between resource availability and CIRP adoption intention among SMEs.	*Rejected*
H4	A positive relationship exists between buyer/suppl. pressure and CIRP adoption intention among SMEs	*Accepted (at p <.1)*
H5	A positive relationship exists between external support and CIRP adoption intention among SMEs.	*Rejected*
H6	A positive relationship exists between tech. uncertainty and CIRP adoption intention among SMEs.	*Rejected*
H7	A positive relationship exists between cyber risk perception and CIRP adoption intention among SMEs.	*Accepted (at p <.01)*

5. Discussion and conclusion

In this chapter, a discussion and conclusion based on the research findings is provided. First, the research findings are interpretated (§5.1). Then, the main research question is answered in the conclusion (§5.2). Subsequently, the theoretical contributions of this study to the literature are discussed (§5.3). Fourth, the practical implications of the research findings are described (§5.4). Finally, the study's limitations are given together with possible directions for future research (§5.5).

5.1 Interpretation of the results

The research findings, as described in the previous chapter, are further interpretated in the following sections on innovation, organizational, environmental and decision maker characteristics.

Innovation characteristics

The research model articulated an expected positive relationship between relative advantage and CIRP adoption intention. Clearly, such positive relationship was not found. Previous researchers have found contrasting results regarding the influence of perceived advantage on adoption of planning-related innovations. Skipper et al. (2009) found that the factor is a significant driver of adoption of contingency planning, while Bandyopadhyay and Schkade (2004) found a non-significant relationship with adoption of disaster recovery planning adoption. However, these findings may not be relevant as they focus on other innovation and contexts. Still, three potential reasons for the unexpected research finding can be discussed. First, perceived advantages from CIRP are perhaps so high that the variable fails to differentiate on CIRP adoption intention, indicated by the relatively high mean of 4.98 and relatively low standard deviation of 0.96. Second, SME decision makers may struggle with assessing the benefits from CIRP as they are not fully knowledgeable about the benefits of using CIRP. Decision makers with little CIRP-knowhow may think that the value of having a plan in place does not surpass the value of a reactive approach. Furthermore, SMEs are required to plan at one point in time, to mitigate unwanted future conditions. Like other preventative innovations (cf. Rogers, 2003; 2002), the advantages of CIRP are only shown when firms need to use their plans. In this regard, decision makers could find it hard to assess how CIRP may benefit their firm in the future. Third, the relative advantage concept of this study may exclude several benefits. As benefits of CIRP can be described in several ways, the measurement of other benefits may potentially differentiate outcomes on the CIRP adoption intention variable.

Organizational characteristics

The research findings further indicated that top management support positively influences CIRP adoption intention among SMEs. This finding is in accordance with previous cybersecurity adoption studies that aim to predict cyber security readiness (Hasan et al., 2021), cybersecurity compliance (Daud, Rasiah, George, Asirvatham & Thangiah, 2018), cybersecurity practices (Kabanda et al., 2018), or information security management (Hsu et al., 2012). Lim, Maynard, Ahmad & Chang (2015) further find that the quality of IT security is higher in firms where top management sees information security as important. The finding suggests that management's vision on how to address cybersecurity and commitment to CIRP adoption is essential, especially in SMEs, to get the adequate resources and support to adopt the innovation. Thereby, prioritization and support for CIRP adoption of upper management must be granted to become more prepared for cyber incidents.

Remarkably, the results show that there is no significant relationship between resource availability and CIRP adoption intention. One possible explanation of this research finding is overconfidence of SME decision makers in handling cyber incidents. Decision makers often consider themselves to have the appropriate expertise, to be well prepared or even immune to cyber incidents (Hoppe et al., 2021). Thereby, they believe that they can easily resolve a possible cyber incident. On the other hand, SMEs are found to often lack basic knowledge and cybersecurity expertise in handling serious cyber incidents. From this perspective, it could be reasoned that deficits in decision makers' knowledge on cyber threats and CIRP make decision makers with less available resources perceive that they have the needed resources to develop a cyber incident response plan, while this is found to be much harder in practice. Subsequently, resource availability is not a differentiating variable.

Environmental characteristics

As related to the environmental characteristics, a positive and significant relationship was found between CIRP adoption intention and buyer/supplier pressure. This implies that SMEs who perceive that they have substantial pressure from consumers or suppliers in their firms' environment are more intended to adopt CIRP. Thereby, this result provides further support for the use of the INT (DiMaggio & Powell, 1983) while emphasizing the relevance of external pressures as influential to adoption of other cybersecurity innovations (cf. Jeyaraj & Zadeh, 2020; Kabanda et al., 2018). Specifically, this

study found that consumers, suppliers, and business partners on average put limited pressure on the sampled SMEs to adopt CIRP, as shown by the relatively low mean of 2.81. Taking this result into consideration, one could suggest that the limited pressure from external parties to adopt CIRP is a possible explanation for low CIRP adoption rates. External parties may not be interested or knowledgeable about cybersecurity issues. However, as this study only identifies coercive pressures from consumer, suppliers and business partners, other types of coercive, mimetic, or normative pressures could be relevant as well. Such pressures are further discussed at the future research directions.

Second, the results show that CIRP adoption intention is not significantly influenced by external support. Hence, external support does not discriminate between the different adopter groups. At least three explanations can be offered as possible causes. First, it is possible that the level of external support for the sampled SMEs is the same, since all these SMEs can tap into the same support resources. From this stance, it must be further noted that the cybersecurity industry is often focused on larger corporations, while neglecting smaller businesses (Osborn, 2015). The limited focus on SMEs consequently could cause that SMEs are not aware of potential support in CIRP. A second possible explanation is that, as already indicated above, SMEs may perceive that developing a cyber incident response plan is simple, think they have the needed expertise, and subsequently think they do not require support from external parties at all. Third, contextual imperatives may have impacted the results. For example, the sampled SMEs may not have a favourable view of vendors in their contexts, while vendors may have difficulties in meeting the specific cybersecurity needs of SMEs.

Unexpectedly, technological uncertainty was found to have a non-significant effect on CIRP adoption intention among the sampled SMEs. One possible explanation for this unexpected result is that uncertainty is a psychological construct that exists more if a person's knowledge is incomplete. Milliken (1987) describes uncertainty as the inability of an individual to forecast something due to lacking information. Perhaps, decision makers (from less technical certain industries) are not aware or knowledgeable about developments regarding IT in their firms' industry. In this regard, they might think that changes occur more or less frequently than other knowledgeable decision makers do. Thus, assessments of technological uncertainty could be made by decision makers that are simply not aware and knowledgeable about changes in IT at their firms' environment.

Decision maker characteristics

Cyber risk perception is found to have a significant and positive effect on CIRP adoption intention. This confirms the idea that risk perceptions of SME decision makers are particularly important for firm-level adoption. The results further show that decision makers think that it is moderately likely that their firm will experience the three scenarios within five years (mean = 5.40). While objective cyber risk exposure levels of each sampled SME cannot be identified, these findings can possibly be placed within previous literature that suggests a gap between cyber risk exposure, cyber risk perception and perceived cyber preparedness (cf. Nam, 2019). In this literature it is described that people underestimate or overestimate risks due to the 'availability heuristic' (De Smidt & Botzen, 2018). According to this heuristic, events are perceived as high risks when it is easy to conceptualize or recall the occurrence of such an event (Tversky & Kahneman, 1973). Thereby, risk perceptions are shaped by recent experiences with risks as well as information about risks from others. From this perspective, Nam (2019) found that managers have higher threat perceptions, but also feel less prepared, as soon as they have recent experiences in, or awareness of cybersecurity breaches. By linking cyber risk perception to CIRP adoption, this study suggest that adequate risk awareness of SME decision makers is key to successful CIRP adoption. Based on the above notions and the PMT (Rogers, 1975), it could be fruitful to test whether cyber risk perception is a mediator of firm cyber experience and CIRP adoption intention among SMEs.

5.2 Conclusion

As cyber incidents proliferate, a SME could develop a cyber incident response plan to be ready to respond. Acknowledging the important social and economic roles of potentially vulnerable SMEs in The Netherlands, the potential of CIRP to mitigate cyber harm for SMEs, and the lack of studies on the adoption of CIRP among firms, a preliminary study on whether and why Dutch SMEs are intended to adopt CIRP becomes relevant. Therefore, this study aims to examine the effects of several innovation, organizational, environmental and decision makers' characteristics on CIRP adoption intention. The main research question is: *Which factors influence CIRP adoption intention among Dutch SMEs?*

To find an answer to the main research question, literature on cybercrime, CIRP and innovation adoption is used. It was found that SMEs could face several cyber-dependent and cyber-enabled crimes, including illegal access to IT-systems, cyber espionage, interference of data and/or IT-systems, cyber

extortion, and financial/internet fraud. These types of cybercrime could cause physical/digital, economic, psychological, reputational, and social/societal harm at SMEs. By seeing CIRP as an innovative tool in management practices that helps to respond to cyber incidents, the underpinnings of four adoption theories – TOE-framework (Tornatzky & Fleischer, 1990), DOI theory (Rogers, 2003), INT (DiMaggio & Powell, 1983), and PMT (Rogers, 1975) – are used to propose a model explaining CIRP adoption intention. Seven hypotheses are suggested, including innovation (*relative advantage*), organizational (*management support, resource availability*), environmental (*buyer/supplier pressure, external support, technological uncertainty*), and decision maker (*cyber risk perception*) characteristics.

The research variables were operationalized by modifying observed variables from previous studies to fit this context and proposing new observed variables where needed. Two IR specialist provided information about CIRP. As well, three marketeers, one SME digital transformation consultant, and one SME owner were asked to provide feedback on the survey. Subsequently, the survey was piloted at three SME owner/managers. Then, data was gathered using an online survey, resulting in 73 usable responses from decision makers in SMEs. Owners, executives, and IT-specialists were targeted because they make decisions to adopt CIRP at their firm. The final research sample included 20 SMEs (27.4%) that have high intention to adopt CIRP, 34 SMEs (46.6%) that have moderate intention to adopt CIRP, and 19 SMEs (26.0%) that have low intention to adopt CIRP or are not intended to adopt CIRP at all. This provides a first indication that firms differ greatly on CIRP adoption intention.

The collected data was input for further quantitative analyses that follows a two-stage approach, differentiating over -measure refinement and validation and -univariate, bivariate and multivariate analyses. To refine and validate the research constructs, a distinction is made between formative, reflective, and single indicator constructs. Different guidelines were followed to validate the formative and reflective constructs of the study (Hair et al., 2014; Field, 2013; Diamantopoulos & Winklhofer, 2001). From the PCA, the five theorized reflective constructs were identified. Then, the five reflective constructs were subject to reliability analyses to enhance internal consistency. For the formative constructs, the content and indicators were specified, and potential multicollinearity issues were identified. In conclusion it can be stated that by conducting the above analytical procedures, the construct validity and reliability of the scales and indexes are enhanced, and substantiated.

After the construct validity and reliability of the scales and indexes are enhanced, the proposed research model was tested. Therefore, hypotheses of the study are accepted or rejected from the results of a OLR analysis. Results show that the proposed research model significantly predicts CIRP adoption intention better than the base model. Based on statistical evidence it was found that top management support is an important driver of CIRP adoption among SMEs. Thereby, *hypothesis 2 is accepted*. Furthermore, a significant and positive relationship is found between buyer/supplier pressure and CIRP adoption. As this provides empirical evidence that *hypothesis 4 is accepted* as well, it can be stated that SMEs that experience more pressure from consumers or suppliers, are found to be more intended to adopt CIRP. Finally, cyber risk perception is found to positively influence CIRP adoption. This result leads to the notion that *hypothesis 7 is accepted*. Thus, when decision makers perceive that their firm is at risk of a cyber incident, it will be more likely that they will be intended to adopt CIRP.

Feeding back to the main research question, this study found one representative, significant variable from organizational, environmental and decision maker characteristic group. More specifically, the three dependent variables 'top management support', 'buyer/supplier pressure' and 'cyber risk perception' have an important role in achieving higher CIRP adoption intention among SMEs in The Netherlands.

5.3 Theoretical contributions

In reaction to the evolving cyber threat landscape, contemporary researchers started to focus on investigating cybersecurity adoption. Despite growing scholarly interest on the adoption of cybersecurity innovations in recent years, most of the current studies are focused on larger corporations, and take a techno-centric, descriptive, or conceptual perspective (Heidt et al., 2019; Hsu et al., 2012). This study contributed to the general cybersecurity adoption literature by conceptualizing and empirically testing an integrative framework predicting CIRP adoption intention among Dutch SMEs. To the researcher's knowledge, this is the first scholarly effort in which CIRP is defined as an innovation, unlocking innovation adoption literature and, subsequently, the CIRP adoption intention and its factors among SMEs is investigated. In this regard, this preliminary study on CIRP adoption intention provides an initial start for the development of specific CIRP adoption literature.

The current study further contributes to the general cybersecurity adoption literature by demonstrating how different theoretical perspectives can be complementary while trying to explain the adoption of a preparative innovation. More specifically, the applicability of three commonly used firm behaviour or innovation adoption theories (TOE-framework, DOI theory and INT) and one individual-level behavioural theory (PMT) in conceptualizing CIRP adoption factors is substantiated. Whereas previous researchers that focus on cybersecurity adoption commonly use one theoretical perspective, this study uses a more holistic view with different theoretical perspectives to propose a research framework with an integrative set of factors, either classified as innovation, organizational, environmental, or decision maker characteristic. Researchers can build on these categories and specific factors while conducting new conceptual or empirical studies focused on CIRP adoption or even building research models for the adoption of other cybersecurity innovations (*see §5.5 for further description of this possible research direction*).

As well, this study offers empirical evidence that SMEs in which (a) the owner and other top managers support the adoption of CIRP, (b) perceive to have more pressure from consumers and/or suppliers, and (c) in which an IT decision maker perceive cyber risks for their firm to be high are more intended to adopt CIRP. Thereby, one representative factor from the organizational, environmental and decision maker group is significant, while no factor from the innovation group is significant. Clearly, this study highlights top management support and cyber risk perception as the most critical factors. Despite these research findings, it is too early to conclude that factors from a specific group are most influential in driving CIRP adoption among SMEs as a different non-comprehensive number of factors were tested in each group. Still, by assessing several possible factors affecting CIRP adoption intention, researchers can differentiate their effects and continue with identifying the most critical factors.

5.4 Practical implications

In addition to the theoretical contributions discussed above, the research findings also have three practical implications for SMEs or other external practitioners promoting CIRP adoption (such as governments, industry associations, interest groups, cybersecurity firms, IT-providers, consultancy firms, and large corporations with SME partners). The three practical implications of this study are described below.

The research findings are beneficial for decision makers in at-risk SMEs that are yet to adopt CIRP because the findings can be used to evaluate significant adoption criteria more fully. Thereby opportunities for successful adoption can be enhanced. First, the study shows that although CIRP is often seen as a low-cost measure with a high impact on cybersecurity (Hoppe et al., 2021), adoption among Dutch SMEs remains very low. At the same time, management support was found to be a driver of CIRP adoption intention. Thus, the underinvestment in CIRP could be seen as an indirect result of prioritizing daily business and short-term temporal focus of SMEs. Decision makers can learn from this finding that seeing CIRP as a strategic priority, creating a broader vision on their firms' cybersecurity, and providing the needed support and resources are time-intensive but important steps for successful CIRP adoption. Thereby, they should question themselves whether they are overemphasizing resource constraints (e.g., limited budget, time, and skilled personnel) as an excuse to delay adoption.

Next, the results implicate that socio-cognitive risk-related aspects deserve further attention since decision makers' cyber risk perceptions are found to affect CIRP adoption intention. Indeed, CIRP should be a strategic imperative to drive adoption, but IT-practitioners in SMEs are also advised to address the central role of cyber risk awareness while building appropriate cybersecurity cultures. Such culture can be defined as: "*the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest themselves in people's behaviour with information technologies"* (ENISA, 2017, p.7). A strong cybersecurity culture exists when individuals are aware and knowledgeable of cyber risks as well as protective measures and take responsibility in performing the required steps to improve their firms' cybersecurity. Developing a cybersecurity culture, while addressing the faulty rationalizations in firms hindering cybersecurity efforts (e.g., 'our firm is too small to be a target of a cybercriminal', 'our firm is well-managed, we will not face cyber incidents', 'it is not possible for us to prepare for cyber incidents', 'executives do not need to be involved since our staff knows how to deal with cyber incidents', 'CIRP is the responsibility of our IT-supplier'; Pearson & Mitroff, 1993 for more faulty rationalizations), could help to foster realistic cyber risk perceptions, which in turn could result in successful CIRP adoption. Vice versa, identifying cyber risks while developing an incident response plan may further establish cybersecurity cultures in firms.

This study also provides external parties that (want to) promote CIRP with relevant insights on how they could drive CIRP adoption intention among SMEs. Although it is found that some SMEs are intended to adopt CIRP after assessing the cyber risks, SMEs could also be pushed by consumers, suppliers, and business partners. To enhance the widespread adoption of CIRP, external actors are advised to pressure SMEs to adopt CIRP. For example, the results indicate that decision makers most often use information from their IT-supplier to inform themselves about cyber threats (*see Appendix E, section 2*). While closing contractual agreements with SME customers regarding their IT-services, the roles and responsibilities for IR should explicitly be assigned. In this regard, IT-suppliers avoid that decision makers think that their IT-supplier is the sole responsible for their firms' cybersecurity and they do not have to prepare themselves. As well, awareness campaigns of governments or industry associations (e.g., MKB-Nederland) should target SME decision makers and the external actors while discussing the collective responsibility of cybersecurity. Finally, in accordance with Heidt et al. (2019) it is advised that large business partners should consider the role of SMEs in their value chains more closely. By seeing SMEs as 'weakest link', corporations are advised to take proactive efforts to ensure that their SME partners are aware of cyber risks and put pressure on SMEs to adopt CIRP.

5.5 Limitations and future research directions

While the research quality of this study is enhanced by several conducted procedures, every study still has its own limitations. Therefore, while who view the results of this study, there are four important limitations that must be considered. By addressing these limitations, several suggestions for future research can be made.

The main limitation of this study relates to the difficulty of generalisation of the findings to a larger population of SMEs. In accordance with other studies at owner/executive level (Yoon & George, 2013; Bednar & Westphal, 2006), it was difficult to collect data from (IT) decision makers in SMEs. Hence, only a small non-random sample could be gathered using convenience sampling methods. The low sample prevented the study from splitting the total dataset into different datasets for analysis, limiting the opportunity to cross-examine the model at specific locations or industries. Furthermore, while it is expected that most of the participating SMEs are in the province of Gelderland (all phone calls were made with firm representatives in this location and the personal contacts of the researcher

live and work in this province), no definite statements regarding location of the SMEs can be made. Thus, because this is the first low sample study on CIRP adoption intention, the research findings should be considered preliminary until confirmed by other studies. Future researchers with more resources (money, time, contacts) are recommended to test the findings across a larger, random sample of Dutch SMEs. When it is possible to collect data from a larger random sample, it is suggested to focus on one or limited number of industries and locations as more validated claims can be made about differences in adoption intention and factors.

Four reasons for the limited response to the survey can be suggested based on the researcher's experiences. First, decision makers may not respond to invitations due to lacking knowledge and interest in CIRP. Hence, they might think that CIRP is irrelevant for their firm and think that CIRP is the responsibility of IT-suppliers. Note that this could also explain the low adoption of CIRP. A second reason is that there was no ready way to collect data through a large, random sample of SMEs. Therefore, SMEs must be approached by phone calls. During these phone calls, receptionists often stated that their firms' decision makers were exceedingly busy and, therefore, lack time to respond. Instead, receptionists often proposed to redirect email invitations. The resulting lack of direct conversations with decision makers formed a participation obstacle. Third, the survey asked for potentially sensitive data. Some decision makers were not enthusiastic about disclosing information about their cyber preparedness and victimization. Despite promises of confidentiality, they might think that disclosure could result in a loss of firm image or customer confidence. Finally, decision makers referred to firm prescriptions against clicking on online survey links from people they do not know or trust. To avoid limited responses among further studies regarding cybersecurity adoption at SME, researchers could consider using a qualitative, case study research strategy in which fewer SMEs need to be approached.

The second limitation of this study is that it uses cross-sectional data, limiting the ability to demonstrate the direction of causality among the variables. This is a frequent limitation in studying adoption (cf. Ghobakhloo & Tang, 2011; Thong, 1999). In cross-sectional studies, surveys are completed by a single respondent at a single point in time (Field, 2013; Rindfleisch, Malter, Ganesan & Moorman, 2008). Thus, for this study, a snapshot of CIRP adoption intention is made. However, adoption is a dynamic process (Rogers, 2003). Decision makers do not decide permanently to adopt

CIRP, but instead make series of decisions: whether to inform themselves about cyber preparation strategies, whether to develop a cyber incident response plan, whether to train employees, among many others. Because this study did not measure the perceptions of the decision makers who are at the same phase in the adoption process, causality between variables can only be inferred, but not proven. A longitudinal study, in which decision makers are followed through the adoption process, is needed to address these dynamics, and test the developed relationships for an extended time. This will help researcher to assess differences in the effects of factors at different adoption phases.

A third limitation of the study, also related to the cross-sectional nature of the data, is that the study uses a single-informant approach for collecting data in each SME. Clearly, these responses may not be representative for entire SMEs. This could result in unwanted bias as perceptions of one decision maker do not necessarily capture internal organizational variety (Van Bruggen, Lilien & Kacker, 2002; Kumar, Stern & Anderson, 1993). While the respondents were all critical decision makers who should be familiar with cybersecurity activities within their firm and directly influence their firms' adoption processes, it is still expected that a single respondent will not be knowledgeable about every cybersecurity adoption-related aspect of their firm. Therefore, it would be preferable to test such expectation in further studies by using multiple respondents for one SME.

Finally, it should be noted that innovation adoption is complex and capturing all its facets in one study is impossible (Damanpour & Schneider, 2006). Therefore, this study might have omitted several factors (and outcomes) of CIRP adoption intention. Due to the lack of CIRP adoption literature, no empirically proven factors of CIRP adoption intention could be used. Therefore, a new model is proposed based on adoption theories proven in other contexts. Future researchers should try to build on this study by developing a more comprehensive model. New predictors can be proposed by utilizing other constructs from the TOE-framework, DOI theory, INT or PMT, but also from adding new adoption theories. For example, researchers could consider other innovation (e.g., *complexity, compatibility, observability, trialability*), organizational (e.g., *IT-capability, organizational culture, centralization, formalization*), environmental (e.g., *governmental pressure/regulations, governmental support, industry standards*) and decision maker characteristics (e.g., *CIRP knowledge, cyber threat knowledge*). Such factors could increase the explained variance of CIRP adoption intention as found in this study.

Adding to the above limitation and avenue for further research regarding factors affecting CIRP adoption intention, the research model can also be extended by adding different adoption stages (intention, adoption decision, implementation) and outcomes of CIRP adoption among SMEs. Drawing on the Resource-Based Theory (Barney, 1991), further studies could investigate the relationship between different CIRP adoption stages, cybersecurity incident response capability and firm performance. CIRP can be seen as a resource of a SME and firm security performance could refer to the overall efficiency and effectiveness of the plan in helping to protect business assets. In this way, the underlying pro-adoption presumption in literature and practice can be addressed: does adopting CIRP indeed help SMEs in dealing more quickly, effective, and efficient with the impact of a cyber incident?

Despite the relevance of the above-mentioned study, expectations are that it is hard to collect a large sample of performance data from large groups of adopter and non-adopter SMEs who experienced cyber incidents. In this regard, Cavusoglu et al. (2015) already stated that firms are reluctant to reveal security performances. If it is possible for researchers to overcome the difficulty of collecting performance data from SMEs, researchers could use the firm security performance construct of Hasan et al. (2021), that includes items about the number of cyber incidents experienced, cybersecurity reputation, system capabilities and database availability. Together, such a study will provide a better understanding of CIRP adoption, the reasons to adopt CIRP, and the consequences of CIRP adoption.

Literature

Ab Rahman, N.H. & Choo, K.K.R. (2015). A survey of information security incident handling in the cloud. *Computer & Security,* Vol.49(1), pp.45-69.

Abed, S.S. (2020). Social commerce adoption using TOE framework: an empirical investigation of Saudi Arabian SMEs. *International Journal of Information Management*, Vol53(1), pp. 1-11.

Abrahamson, E. (1991). Managerial Fads and Fashions: The Diffusion and Rejection of Innovations. *Academy of Management Review,* Vol.16(3), pp.586-612.

Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S. & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity,* Vol. 4(1), pp. 1-15

Aguilar, L. A. (2015). The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses. Accessed on June 7, 2022, at: https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html

Ahmad, A., Hadjkiss, J. & Ruighaver, A.B. (2012). Incident response teams – Challenges in supporting the organizational security function. *Computer & Security,* Vol.31(5), pp.643-652.

American Psychological Association. (2017). Ethical principles of psychologist and code of conduct. Accessed on June 7, 2022, at: https://www.apa.org/ethics/code/

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M.J.G., Levi, M., Moore, T. & Savage, S. (2014). Measuring the Cost of Cybercrime. In: Böhme, R. (Ed.). *The economics of information security and privacy* (pp.265-300). New York: Springer.

Awa, H.O., Ukoha, O., Emecheta, B.C. & Liu, S. (2016). Using T-O-E theoretical framework to study the adoption of ERP solution. *Cogent Business & Management,* Vol.3(1), pp.1-23.

Bada, M. and Nurse, J.R.C. (2019). Developing cybersecurity education and awareness programmes for small and medium-sized enterprises (SMEs). *Information and Computer Security*, Vol. 27(3), pp. 393-410.

Baker, J. (2011). The technology-organization-environment framework. In: Dwivedi, Y., Wade, M. & Schneberger, S. (Eds.) Information System Theory: Explaining and predicting our digital society, pp. 231-246. New York: Springer.

Bandyopadhyay, K. & Schkade, L.L. (2000). Disaster recovery planning by HMOs: theoretical insights. *HealthCare Management Review,* Vol.25(2), pp. 74–84.

Bandyopadhyay, K. & Schkade, L.L. (2004). Initiation, adoption, and implementation of disaster recovery planning by health maintenance organizations. *International Journal of Internet and Enterprise Management,* Vol.2(4), pp.309-340.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management,* Vol. 17(1), pp.99-120.

Bednar, M.K. & Westphal, J.D. (2006). Surveying the corporate elite: theoretical and practical guidance on improving response rates and response quality in top management survey questionnaires. In: Ketchen, D.J. Jr and Bergh, D.D. (eds.) *Research Methodology in Strategy and Management*, pp 37-55. Amsterdam: Elsevier.

Benz, M. & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons,* Vol.63(4), pp.531-540.

Barlette, Y., Gundolf, K. & Jaouen, A. (2017). CEOs' information security behavior in SMEs: Does ownership matter? *Systèmes d'Information et Management,* Vol.22(3), pp.7-45.

Bstieler, L. (2005). The moderating effect of environmental uncertainty on new product development and time efficiency. *Journal of Product Innovation Management,* Vol.22(3), pp.267-284.

Carmelli, A. & Schaubroeck, J. (2008). Organisational Crisis-Preparedness: The Importance of Learning from Failures. *Longe Range Planning*, Vol.41(2), pp. 177-196.

Cavusoglu, H., Cavusoglu, H., Son, J., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management,* Vol.52(4), pp.385-400

Central Bureau of Statistics. (2021). *Cybersecuritymonitor 2020*. The Hague: Central Bureau of Statistics.

Central Bureau of Statistics. (2022). StateLine MKB. Accessed on June 7, 2022, at: https://mkbstatline.cbs.nl/#/MKB/nl/dataset/48034NED/table?ts=1652178500405

Chang, I. C., Hwang, H. G., Hung, M. C., Lin, M. H., & Yen, D. C. (2007). Factors affecting the adoption of electronic signature: Executives' perspective of hospital information department. *Decision Support Systems*, vol.44(1), pp. 350–359.

Choo, K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computer & Society.* Vol. 30(8), pp. 719-731

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide.* Gaithersburg: NIST Special Publications.

Coombs, T. W. (2014). *Ongoing crisis communication: planning, managing, and responding*. (4th Edition). Thousand Oaks, California: Sage Publications.

Corey, C.M. and Deitch, E.A. (2011). Factors affecting business recovery immediately after Hurricane Katrina. *Journal of Contingencies and Crisis Management*, Vol. 19(3), pp. 169-181.

Crane, A. (2005). In the company of spies: When competitive intelligence gathering becomes industrial espionage. *Business Horizons,* Vol.48(3), 233-240.

Creswell, J.W. (2014). *Research design: qualitative, quantitative, and mixed methods approaches.* Thousand Oaks, California: SAGE Publications.

Cyber Security Council. (2021). *Adviesrapport. Integrale aanpak cyberweerbaarheid.* The Hague: Cyber Security Council.

Daft, R.L. & Weick, K.E. (1984). Towards a model of organizations as interpretations systems, *Academy of Management Review,* Vol.9(2), pp.284-295.

Damanpour, F. & Gopalakrishnan, S. (1998). Theories of organizational structure and innovation adoption: the role of environmental changes. *Journal of Engineering and Technology Management,* Vol.15(1), pp.1-24.

Damanpour, F. & Schneider, M. (2006). Phases of the adoption of innovation in organizations: Effects of environment, organization, and top managers. *British Journal of Management*, Vol.17(3), pp.215-236.

Data Protection Authority. (2021). *Meldplicht datalekken: facts & figures. Overzicht feiten en cijfers 2020*. The Hague: Data Protection Authority.

Daud, M., Rasiah, R., George, M., Asirvatham, D. & Thangiah, G. (2018). Bridging the gap between organizational practices and cyber security compliance: Can cooperation promote compliance in organisations? *International Journal of Business and Society,* Vol.19(1), pp.161-180.

De Cuyper, R.H. & Weijters, G. (2016). *Cybercrime in numbers: Exploring the possibilities to include cybercrime in the National Security Indices*. The Hague: WODC.

De Smidt, G. & Botzen, W. (2018). Perceptions of corporate cyber risks and insurance decision-making. *The Geneva Papers on Risk and Insurance-Issues and Practice,* Vol.43(2), pp.239-274.

Deloitte. (2016). Cyber Value at Risk in the Netherlands. Amsterdam, The Netherlands: Deloitte.

Diamantopoulos, A. & Siguaw, J. (2006). Formative versus reflective indicators in organizational measure development: a comparison and empirical illustration. *British Journal of Management,* Vol.17(4), pp. 263–82.

Diamantopoulos, A. & Winklhofer, H.M. (2001). Index construction with formative indicators: An alternative to scale development. *Journal of Marketing Research,* Vol.38(2), pp.269-277.

DiMaggio P, Powell W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, Vol.48(2), pp.147–160

Elsubbaugh, S., Fildes, R., & Rose, M. (2004). Preparation for crisis management: A proposed model and empirical evidence. *Journal of Contingencies and Crisis Management*, Vol.12(3), pp. 112-127.

European Network and Information Security Agency. (2021a). *ENISA Threat Landscape 2021.* Heraklion, Greece: European Network and Information Security Agency.

European Network and Information Security Agency. (2021b). *Cybersecurity for SMEs: Challenges and Recommendations.* Heraklion, Greece: European Network and Information Security Agency.

European Network and Information Security Agency. (2017). *Cyber security culture in organizations*. Heraklion, Greece: European Network and Information Security Agency.

European Commission. (2015). User Guide to the SME Definition. Accessed on June 7, 2022, at http://ec.europa.eu/DocsRoom/documents/15582/attachments/1/translations

Eurostat. (2022). Digital economy and society statistics – enterprises. Accessed on June 7, 2022, at https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_enterprises#Access_and_use_of_the_internet (Accessed: May 9, 2022).

Field, A. (2013). *Discovering statistics using IBM SPSS statistics* (4th ed.). London: SAGE.

Fielder, A., Panaousis, E. Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision Support Approaches for Cyber Security Investment. *Decision Support Systems* Vol.86(3), pp.13–23

Frambach, R.T. & Schillewaert, N. (2002). Organization innovation adoption. A multi-level framework of determinants and opportunities for future research. *Journal of Business research,* Vol.55(2), pp.163-176.

Ghobakhloo, M., Arias-Aranda, D., & Benitez-Amado, J. (2011). Adoption of E-Commerce Applications in SMEs. *Industrial Management & Data Systems,* Vol.111(8), pp.1238–1269.

Ghobakhloo, M. & Ching, N.T. (2019). Adoption of digital technologies of smart manufacturing in SMEs. *Journal of Industrial Information Integration,* Vol.16(1), pp.100-107.

Ghobakhloo, M. & Tang, S.H. (2011). Barriers to Electronic Commerce Adoption Among Small Businesses in Iran. *Journal of Electronic Commerce in Organizations,* Vol.9(4), pp.48-89.

Grabosky P. (2016). The evolution of cybercrime, 2006–2016. In: Cybercrime Through an Interdisciplinary Lens, ed. TJ Holt, pp. 15–37. New York: Routledge

Greenhalgh, T., Robert, G., Macfarlane, F., Bate, P., & Kyriakidou, O. (2004). Diffusion of innovations in service organizations: Systematic review and recommendations. *Milbank Quarterly*, Vol. 82(4), pp. 581–629.

Grover, V. & Goslar, M.D. (1993). The Initiation, Adoption, and Implementation of Telecommunications Technologies in U.S. Organizations. *Journal of Management Information Systems,* Vol.10(1), pp. 141-164.

Hair, J.F., Black, W.C., Babin, B.J. & Anderson, R.E. (2014). *Multivariate Data Analysis* (7th ed.). Upper Saddle River: Pearson Education.

Hameed, M.A., Counsell, S. & Swift, S. (2012). A conceptual model for the process of IT innovation adoption in organizations. *Journal of Engineering and Technology Management,* Vol.29(3), pp.358-390.

Han, Z. & Nigg, J. (2011). The influences of business and decision makers' characteristics on disaster preparedness – a study on the 1989 Loma Prieta earthquake. *Internation Jounal of Disaster Risk Science,* Vol.2(4), pp. 22-31.

Harsch, A., Idler, S. & Thurner, S. (2014). Assuming a state of compromise: A best practice approach for SMEs on incident response management. *Proceedings of the Eight International Conference on IT Security Incident Management & IT Forensics (IMF 2014),* IEEE Computer Society, Munster*,* pp. 76-84.

Hasan, S., Ali, M., Kurnia, S. & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications,* Vol. 58(4), pp. 1-16.

Hayes, J. & Bodhani, A. (2013). Cyber security: small firms under fire. *Engineering Technology*, Vol. 8(6), pp. 80–83.

Heidt, M., Gerlach, J.P. & Buxmann, P. (2019). Investigating the Security Divide between SME and Large Companies: How SME characteristics Influence Organizational IT Security Investments. *Information Systems Frontiers,* Vol.21(6), pp.1285-1305

Herbane, B. (2010). Small business research: Time for a crisis-based view. *International Small Business Journal,* Vol.28(1), pp.43-64.

Herbane, B. (2015). Threat orientation in small and medium enterprises – Understanding differences toward acute interruptions. *Disaster Prevention and Management,* Vol.24(5), pp. 583-595

Holt, T.J. & Bossler, A.M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior,* Vol. 35(1), pp. 20-40.

Holt, T.J. & Bossler, A.M. (2016). *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses.* New York: Routledge.

Hoppe, F., Gatzert, N. & Gruner, P. (2021). Cyber risk management in SMEs: insights from industry surveys. *The Journal of Risk Finance,* Vol.22(3/4), pp.240-260.

Hosmer, D.W. & Lemeshow, S. (2000). *Applied Logistic Regression* (2nd ed.). New York: Wiley

Howe, P.D. (2011) Hurricane preparedness as anticipatory adaptation: a case study of community businesses. *Global Environmental Change,* Vol.21(2), pp.711-720.

Hsu, C., Lee, J. & Straub, D.W. (2012). Institutional influences on information systems security innovations. *Information Systems Research,* Vol.23(3), pp.918-939

Hutcheson, G. & Sofroniou, N. (1999). *The Multivariate Social Scientist: Introductory Statistics Using Generalized Linear Models.* Thousand Oaks, California: Sage Publication.

Ifinedo, P. (2011). An Empirical Analysis of Factors Influencing Internet/E-Business Technologies Adoption by SMEs in Canada. *International Journal of Information Technology and Decision Making,* Vol.10(4), pp. 731-766.

Jarvis, C.B., MacKenzie, S.B. & Podsakoff, P.M. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of Consumer Research,* Vol.30(2), pp.199-218.

Jeyaraj, A. & Zadeh, A. (2020). Institutional Isomorphism in Organizational Cybersecurity: A Text Analytics Approach. *Journal of Organizational Computing and Electronic Commerce,* Vol.30(4), pp. 1-21.

Kabanda, S., Tanner, M. & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce,* Vol.28(3), pp.269-282

Kaiser, H. F. (1960). The application of electronic computers to factor analysis. *Educational and Psychological Measurement*, Vol.20(1), pp. 141–151.

Kim, L.L. & Amran, A. (2018). Factors leading to the adoption of business continuity management (BCM) in Malaysia. *Global Business and Management Research: An International Journal,* Vol.10(1), pp.179-196

Kral P. (2011). *Incident handler handbook.* Accessed on June 7, 2022, at: https://www.sans.org/white-papers/33901/

Kumar, N., Stern, L.W. & Anderson, J.C. (1993). Conducting interorganizational research using key informants. *Academy of Management Journal,* Vol.36(6), pp.1633-1651.

Land, S., Engelsen, A. & Brettel, M. (2012). Top management's social capita land learning in new product development and its interaction with external uncertainties. *Industrial Marketing Management,* Vol.41(3), pp.521-530.

Lee, E., Kwon, K. & Schuman, D.W. (2005). Segmenting the non-adopter category in the diffusion of internet banking. *International Journal of Bank Marketing,* Vol.23(5), pp.414-437.

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,* Vol.18 (2), pp. 177–187.

Leukfeldt, R. (2021). *Van theorie naar praktijk: De geleerde lessen van 4 jaar onderzoek naar cybersecurity in het mkb.* The Hague: De Haagse Hogeschool.

Lezzi, M., Lazoi, M. & Coralla, A. (2018). Cybersecurity for industry 4.0 in the current literature: A reference framework. *Computers in Industry*, Vol.103(10), pp. 97–110.

Lian, J., Yen, D.C. & Wang, Y. (2014). An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. *International Journal of Information Management,* Vol.34(1), pp. 28-36

Liang, H., Saraf, N. & Hu, Q. (2007). Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management. *MIS Quarterly,* Vol.31(1), pp.59-87.

Lim, J.S., Maynard, S.B., Ahmad, A. & Chang, S. (2015). Information security culture. Towards an instrument for assessing security management practices. *International Journal of Cyber Warfare and Terrorism*, Vol. 5(2), pp. 31-52.

Maduku, D.K., Mpinganjira, M. & Duh, H. (2016). Understanding mobile marketing adoption intention by South African SMEs: A multi-perspective framework. *International Journal of Information Management,* Vol. 36(5), pp.711-723.

Maimon, D. & Louderback, E. R. (2019). Cyber-Dependent Crimes: An interdisciplinary Review. *Annual Review of Criminology*, Vol.2(1), pp. 191-216.

Maj, M., Reijers, R., & Stikvoort, D. (2010). Good practice guide for incident management. European network and information security agency (ENISA).

Maroufkhani, P., Tseng, M., Iranmanesh, M., Khairuzzaman, W., Ismail, W. & Khalid, H. (2020). Big data analytics adoption: Determinants and performance among small and medium-sized enterprises. *International Journal of Information Management,* Vol. 54(3), pp. 1-15.

McConnell, A., & Drennan, L. (2006). Mission Impossible? Planning and Preparing for Crisis. *Journal of Contingencies and Crisis Management*, Vol.14(2), 59-70.

McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence.* London: Home Office.

Memon, G., Raghubir, P. & Agrawal, N. (2008). Health risk perceptions and consumer psychology. In: Haugtvedt, C.P., Herr, P.M. & Kardes, F.R. (Eds.). *Handbook of consumer psychology*, pp.981-1010. New York, NY: Laurence Erlbaum.

Miller, D. & Friesen, P.H. (1982). Innovation in conservative and entrepreneurial firms: Two models of strategic momentum. *Strategic Management Journal,* Vol.3(1), p.1-25.

Milliken, F.J. (1987). Three types of perceived uncertainty about the environment: State, effect, and response uncertainty. *Academy of Management Review,* Vol.12(1), pp. 133-143.

Morreale, T. (2008). *Incident handling for SMEs (Small to Medium Enterprises)*. Accessed on June 7, 2022, at: https://www.sans.org/white-papers/32764/

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity, *Technology in Society*, Vol. 58, (article 101122), pp.1-10.

National Coordinator for Security and Counterterrorism. (2020). *Cybersecuritybeeld Nederland: CSBN 2020*. National Coordinator for Security and Counterterrorism: Den Haag

National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments.* National Institute of Standards and Technology: Gaithersburg.

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. National Institute of Standards and Technology: Gaithersburg.

Nunnally, J.C. (1978). *Psychometric theory* (2nd ed.). New York: McGraw-Hill.

Oliveira, T. & Martins, M.F. (2010). Understanding e-business adoption across industries in European countries. *Industrial Management & Data Systems,* Vol.110(9), pp.1337-1354.

Osborn, E. (2015). Business versus Technology: Sources of the Perceived Lack of Cyber Security in SMEs. Accessed on June 7, 2022, at: https://ora.ox.ac.uk/catalog/uuid:4363144b-5667-4fdd-8cd3-b8e35436107e/download_file?file_format=application%2Fpdf&safe_filename=01-15.pdf

Osborne, J.W. (2015). *Best Practices in Logistic Regression.* Thousand Oaks, California: SAGE Publications.

Ottis, R. & Lorents, P. (2010). Cyberspace: Definition and Implications. *Proceedings of 5th International Conference on Information Warfare and Security*, pp. 267-270.

Paoli, L., Visschers, J. & Verstraete., C. (2018). The impact of cybercrime on businesses: a novel conceptual framework and its application to Belgium. *Crime Law and Social Change,* Vol.70(4), pp. 397-420.

Payne B.K. (2019) Defining Cybercrime. In: Holt T., Bossler A. (eds). *The Palgrave Handbook of International Cybercrime and Cyberdeviance.* London: Palgrave Macmillan, Cham.

Pearson, C.M. & Mitroff, I.I. (1993). From crisis prone to crisis prepared: a framework for crisis management. *Academy of Management Executive,* Vol.7(1), pp.48-59.

Petter, S. & Straub, D., & Raj, A. (2007). Specifying formative constructs in information system research. *MIS Quarterly,* Vol.31(4), pp.623-656.

Pfeffer, J. & Salancik, G.R. (1978). *The External Control of Organizations: A Resource Dependence Perspective.* New York: Harper & Row.

Podsakoff, N.P., Shen, W. & Podsakoff, P.M. (2006). The role of formative measurement models in strategic management research : Review, critique, and implications for further research. *Research Methodology in Strategy and Management,* Vol.3, pp.197-252.

Ponsard, C., Grandclaudon, J. & Dallons, G. (2018). Towards a Cyber Security Label for SMEs: A European Perspective. *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*, pp. 426-431.

Preble, J. F. (1997). Integrating the crisis management perspective into the strategic management Process. *Journal of Management Studies*, Vol. 34(5), pp. 769-791.

Premkumar, G. & Roberts, M. (1999). Adoption of new information technologies in rural small businesses. *Omega, International Journal of Management Science,* Vol.27(4), pp. 467-484.

Ramdani, B., Kawalek, P. & Lorenzo, O. (2009). Predicting SMEs' adoption of enterprise systems. *Journal of Enterprise Information Management,* Vol.22(1/2), pp. 10-24.

Reilly, A.H. (1993). Preparing for the worst: The process of effective crisis management. *Industrial and Environmental Crisis Quarterly*, Vol.7(2), pp. 115–143.

Rindfleisch, A., Malter, A.J., Ganesan, S. & Moorman, C. (2008). Cross-Sectional Versus Longitudinal Survey Research: Concepts, Findings and Guidelines. *Journal of Marketing Research,* Vol. 45(3), pp.261-279

Ritchie, B.W., Bentley, G. Koruth, T. & Wang, J. (2011). Proactive crisis planning: Lessons for the accommodation industry. *Scandinavian Journal of Hospitality and Tourism,* Vol. 11(3), pp.367-386.

Rogers, E.M. (2003). *Diffusion of Innovations (5th edition)*. New York: Free press.

Rogers, E.M. (2002). Diffusion of preventive innovations. *Addictive Behaviors,* Vol.27(6), pp. 989-993.

Rogers, R.W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology*, Vol.91(1), pp. 93-114

Runyan, R.C. (2006). Small Business in the Face of Crisis: Identifying Barriers to Recovery from a Natural Disasters. *Journal of Contingencies and Crisis Management,* Vol.14(1), pp. 12-26.

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

Saleem, J., Adebisi, B., Ande, R. and Hammoudeh, M. (2017). A state-of-the-art survey - impact of cyber attacks on SME's. *Proceedings of the International Conference on Future Networks and Distributed Systems (ICFNDS),* Cambridge, UK; Art. No. 52.

Sheaffer, Z. & Mano-Negrin, R. (2003). Executives' orientations as indicators of crisis management policies and practices, *Journal of Management Studies*, Vol. 40(2), pp. 573-606.

Skipper, J.B., Hanna, J.B. & Cegielski, C.G. (2009). Supply chain contingency planning and firm adoption: An initial look at differentiating the innovators. *Transportation Journal,* Vol.48(2), pp.40-62.

Søilen, K.S. (2016). Economic and industrial espionage at the start of the 21st century – Status quaestionis. *Journal of Intelligence Studies in Business,* Vol. 6(3), pp. 51-64.

Sophonthummapharn, K. (2009). The adoption of techno-relationship innovations. *Marketing Intelligence & Planning,* Vol.27(3), pp. 380-412.

Spillan, J. & Hough, M. (2003). Crisis Planning in Small Businesses: Importance, Impetus and Indifference. *European Management Journal,* Vol.21(3), pp.398-407.

Suchman, M. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review,* Vol.20(3), pp.571-610.

Sultan, F. & Chan, L. (2000) The adoption of new technology: the case of object-oriented computing in software companies. *IEEE Transactions on Engineering Management*, Vol. 47(1), pp. 106–126.

Tan, K.S., Eze, U.C. and Chong, S.C. (2009). Factors influencing internet-based information and communication technologies adoption among Malaysian small and medium enterprises. *International Journal of Management and Enterprise Development*, Vol. 6(4), pp. 397-418.

Teo, H.H., Wei, K.K. and Benbasat, I. (2003). Predicting intention to adopt interorganizational linkages: an institutional perspective. *MIS Quarterly*, Vol. 27(1), pp.19-49.

Terawantanavong, C., Whitwell, G.J., Widing, R.E. & O'Cass, A. (2011). Technological turbulence, supplier market orientations, and buyer satisfactions. *Journal of Business Research,* Vol.64(8), pp.911-918.

Thong, J.Y.L. (1999). An integrated model of information systems adoption in small businesses. *Journal of Management Information Systems*, Vol.15(4), pp. 187–214.

Tornatzky, L.G. & Fleischer, M. (1990). *The Process of Technology Innovation.* Lexington: Lexington Books.

Tversky, A. & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. *Cognitive Psychology,* Vol.5(2), pp. 207-232.

Van Bruggen, G. H., Lilien, G.L. & Kacker, M. (2002). Informants in organizational marketing research: Why use multiple informants and how to aggregate responses. *Journal of Marketing Research,* Vol.39(4), pp. 469–478.

Van Thiel, S. (2014). *Research in Public Administration and Public Management: An Introduction, Routledge Masters in Public Management*. London: Routledge.

Verhees, F.J.H.M., Meulenberg, M.T.G. (2004). Market orientation, innovativeness, product innovation and performance in small firms. *Journal of Small Business Management,* Vol.42(2), pp. 134-154.

Wall, D.S. (2001). Cybercrimes and the Internet. In: Wall, D.S. (Ed.). *Crime and the Internet*, p.1-14. New York: Routledge.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Malden: Polity Press.

Yoon, T.E. & George, J.F. (2013). Why aren't organization adopting virtual worlds? *Computers in Human Behavior,* Vol.29(3), pp. 772-790.

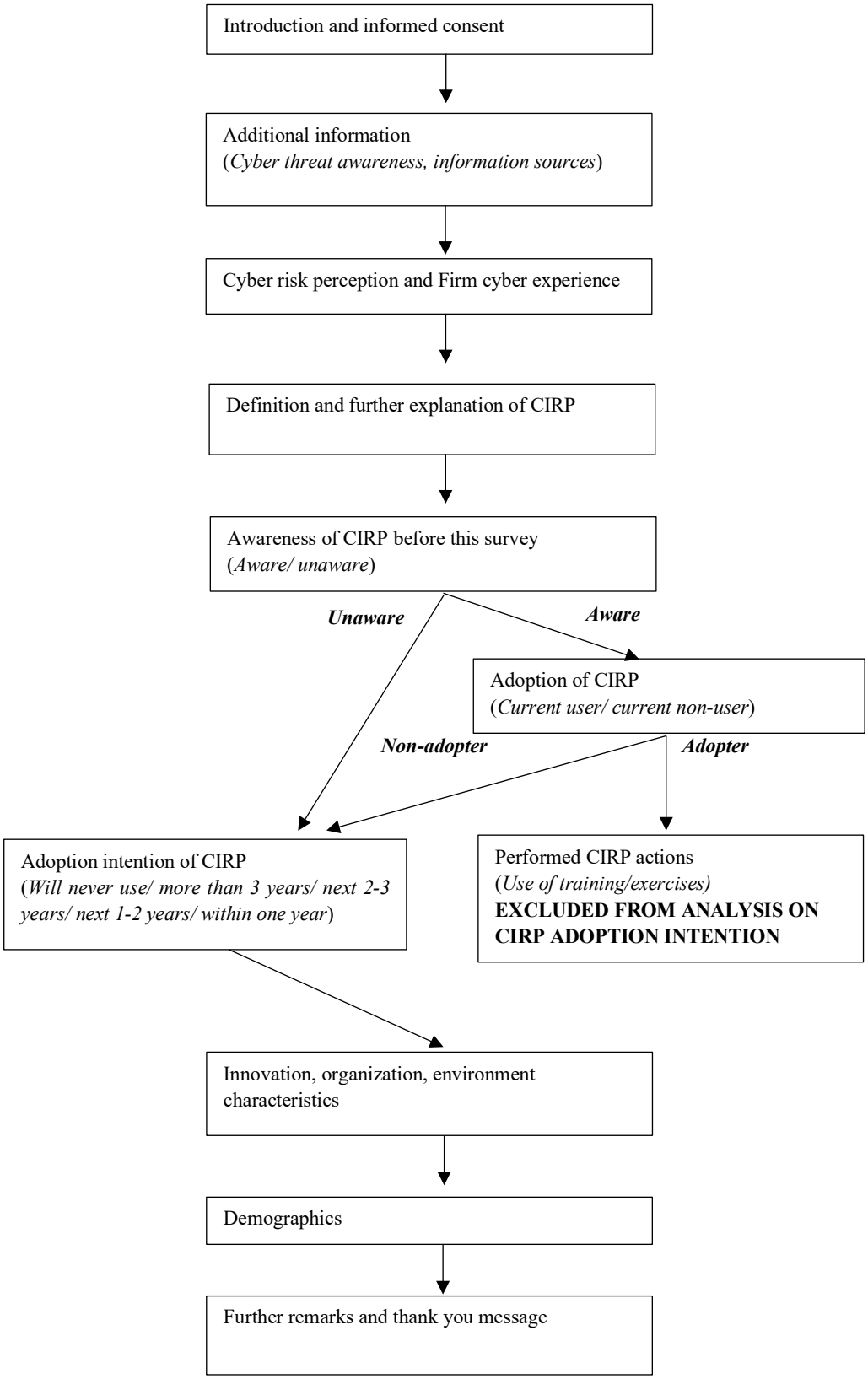
Appendix A – Operationalization of the variables

Table 9 –Operational measures of variables (= eliminated after scale purification)*

Variable	Item(-s)	Response scale	Measurement	Inspired by/ adapted from:
CIRP adoption	Indication how firms are intended to adopt CIRP	3 ordinal categories after treatment (1=no/low intention, 2=moderate intention, 3=high intention)	Single indicator	
Perceived relative advantage	ADV1 – CIRP enables our firm to lessen damage towards organizational reputation ADV2 – CIRP can shorten the duration of business interruptions for our firm (*) ADV3 – CIRP can lessen the magnitude of lost revenue for our firm ADV4 – CIRP can avoid legal exposure for our firm, such as fines, claims and other compensation costs ADV5 – CIRP can lessen the recovery cost for IT-systems and data that are damaged due to cyber incidents ADV6 – CIRP can lessen cost for personnel (internal/external) that needs to neutralize cyber incidents in our firm	7-point Likert scale (1=strongly disagree, 7=strongly agree)	Reflective	Advantages of CIRP inspired by Bandyopadhyay & Schkade (2004) and cyber harm types from Paoli et al. (2018) and Agrafiotis et al. (2020)
Top management support	TOP1 – Top management is aware of the benefits of CIRP TOP2 – Top management considers the adopting of CIRP as strategically important TOP3 – Top management provides the necessary support the adoption of CIRP TOP4 – Top management provides adequate resources for adopting CIRP	7-point Likert scale (1=strongly disagree, 7=strongly agree)	Reflective	Maroufkhani et al., (2020) ; Lian et al., (2014); Premkumar & Roberts, (1999);
Resource availability	RES1 – Firm has the capital (money) needed for the adoption of CIRP RES2 – Firm has the organizational time needed for the adoption of CIRP RES3 – Firm has skilled people needed for the adoption of CIRP	7-step Likert scale (1=strongly disagree, 7=strongly agree)	Formative	Miller & Friesen (1982)
Buyer/supplier pressure	PRE1 – Our industry is pressuring us to adopt CIRP (*) PRE2 – Our customers are pressuring us to adopt CIRP PRE3 – Our suppliers are pressuring us to adopt CIRP PRE4 – Our distant partners' cybersecurity demands are pressuring us to adopt CIRP	7-point Likert scale (1=strongly disagree, 7=strongly agree)	Reflective	Ghobakhloo et al. (2011); Premkumar & Roberts (1999)

External support	SUP1 – Vendors actively market CIRP SUP2 – There are adequate support for CIRP provided by vendors SUP3 – Training for CIRP is adequately provided by vendors	7-point Likert scale (1=strongly disagree, 7=strongly agree)	Reflective	Ghobakhloo et al. (2011); Premkumar & Roberts (1999)
Technological uncertainty	TEC1 – IT in our industry is always changing TEC2 – There are frequent changes in IT use by our firm TEC3 – Our firm changes IT capability frequently (*)	7-point Likert scale (1=strongly disagree, 7=strongly agree)	Reflective	Bandyopadhyay & Schkade (2004)
Cyber risk perception	Please rate the probability that your firm must deal with the cyber scenarios, within the following five years: RIS1 – CEO-FRAUD RIS2 – RANSOMWARE AND CYBER EXTORTION RIS3 – (DISTRIBUTED) DENIAL-OF-SERVICE ATTACK	11-point Likert scale (1=not likely at all, 11=extremely likely)	Formative	Cyber scenarios based on business-related cybercrime conceptualization of Paoli et al. (2018)
Firm size	The current number of firm employees (In FTE)	(Categories: 1=micro 2-9fte, 2=small 10-49fte, 3=medium 50-249fte)	Single indicator per category	n/a
Firm industry (Information & Communication)	The firm is primarily active in the Information and Communication industry	Dummy variable (1=yes, 0=no)	Single indicator	n/a

Appendix B – Routing of the survey



Appendix C – SPSS output: Principal component analysis

Section 1. Assumptions before conducting an initial PCA – Anti-image matrix

	ADV1	ADV2	ADV3	ADV4	ADV5	ADV6	TOP1	TOP2	TOP3	TOP4	PRE1	PRE2	PRE3	PRE4	SUP1	SUP2	SUP3	TEC1	TEC2	TEC3
ADV1	**.643**																			
ADV2	-.085	**.696**																		
ADV3	.040	-.559	**.734**																	
ADV4	-.724	.115	-.289	**.681**																
ADV5	-.244	.065	-.226	.199	**.750**															
ADV6	.197	-.046	-.086	-.268	-.425	**.813**														
TOP1	.236	-.106	-.091	-.164	.143	.204	**.737**													
TOP2	-.051	.011	-.033	.042	-.205	-.268	-.549	**.758**												
TOP3	.091	-.128	.196	-.056	.067	.093	-.046	-.315	**.807**											
TOP4	-.144	-.122	.112	.118	.026	-.178	-.217	-.151	-.210	**.877**										
PRE1	.180	.017	.054	-.167	-.076	-.002	.026	.070	-.271	-.013	**.857**									
PRE2	.092	.206	-.168	-.061	-.142	.061	-.135	.189	-.118	-.124	-.144	**.845**								
PRE3	-.044	-.283	.245	.055	.137	.060	.279	-.424	.284	.124	-.449	-.351	**.722**							
PRE4	-.097	.037	.002	-.033	-.065	-.189	-.259	.285	-.139	.074	.270	-.397	-.552	**.771**						
SUP1	.117	.033	-.217	-.013	.139	.142	.029	.048	-.182	-.067	.024	.137	.032	-.355	**.780**					
SUP2	-.082	.141	.054	-.038	.000	.006	.073	-.238	.141	.113	-.155	-.155	.143	.119	-.553	**.739**				
SUP3	-.183	-.026	-.016	.187	-.123	-.115	-.091	.115	-.031	-.117	-.054	.119	-.184	.101	-.307	-.421	**.879**			
TEC1	-.069	-.172	-.012	.092	.106	.027	-.120	.100	-.027	-.213	.035	.033	-.001	-.100	.341	-.387	.017	**.712**		
TEC2	.106	.159	-.074	-.071	-.113	-.030	.082	-.019	.097	-.007	-.199	.029	-.020	.089	-.303	.394	-.097	-.711	**.676**	
TEC3	-.019	.108	.049	-.042	.181	-.049	.173	-.218	.014	.078	-.139	.091	.213	-.321	.071	.052	-.072	-.094	-.289	**.757**

Notes: Individual KMO-measures of sampling adequacy are bold on the diagonal, partial correlations on the off-diagonal

Section 2. Assumptions before conducting an initial PCA – Inter-item correlations and sampling adequacy

	ADV1	ADV2	ADV3	ADV4	ADV5	ADV6	TOP1	TOP2	TOP3	TOP4	PRE1	PRE2	PRE3	PRE4	SUP1	SUP2	SUP3	TEC1	TEC2	TEC3
ADV1	**1.000**																			
ADV2	.235*	**1.000**																		
ADV3	.442**	.601**	**1.000**																	
ADV4	.763**	.251*	.536**	**1.000**																
ADV5	.435**	.271*	.488**	.367**	**1.000**															
ADV6	.376**	.338**	.481**	.466**	.665**	**1.000**														
TOP1	-.007	.401**	.303**	.154	.098	.215*	**1.000**													
TOP2	.162	.384**	.309**	.229*	.372**	.497**	.678**	**1.000**												
TOP3	-.084	.212*	.033	.036	.016	.136	.558**	.566**	**1.000**											
TOP4	.098	.367**	.229**	.110	.217*	.359**	.599**	.617**	.549**	**1.000**										
PRE1	.050	.095	.030	.178	.169	.268*	.225*	.396**	.429**	.295**	**1.000**									
PRE2	.172	.138	.155	.294**	.234*	.283**	.287**	.290**	.320**	.210*	.634**	**1.000**								
PRE3	.172	.203*	.066	.233*	.195*	.290**	.201*	.356**	.269*	.176	.723**	.835**	**1.000**							
PRE4	.251*	.189	.192	.349**	.224*	.340**	.291**	.298**	.313**	.203*	.585**	.854**	.853**	**1.000**						
SUP1	.167	.113	.247*	.203*	.133	.189	.312**	.376**	.414**	.313**	.506**	.453**	.471**	.551**	**1.000**					
SUP2	.257*	.068	.211*	.219*	.210*	.231*	.281**	.434**	.329**	.315**	.463**	.351**	.356**	.374**	.814**	**1.000**				
SUP3	.267*	.176	.258*	.202	.297**	.336**	.303**	.461**	.361**	.412**	.532**	.380**	.452**	.444**	.796**	.821**	**1.000**			
TEC1	.088	.206*	.161	.115	.107	.254*	.284**	.321**	.261*	.461**	.423**	.237*	.284**	.306**	.275**	.314**	.401**	**1.000**		
TEC2	.034	.058	.124	.117	.139	.266*	.116	.224*	.173	.311**	.475**	.227*	.298**	.304**	.289**	.184*	.356**	.791**	**1.000**	
TEC3	.074	-.087	-.016	.147	.011	.203*	.025	.177	.151	.145	.377**	.198*	.252*	.335**	.212*	.149	.250*	.522**	.623**	**1.000**

Notes: *Significant at .05 level (1-tailed), **Significant at .01 level (1-tailed). Overall KMO-measure of sampling adequacy = .767, Bartlett's Test of Sphericity (df=190) = 1033.906 significant at <.001.

Section 3. Initial analysis – Results for the extraction of components before scale purification

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	6.989	34.944	34.944	6.989	34.944	34.944	3.321	16.607	16.607
2	2.658	13.289	48.233	2.658	13.289	48.233	3.265	16.326	32.933
3	2.100	10.498	58.732	2.100	10.498	58.732	3.141	15.707	48.640
4	1.754	8.770	67.502	1.754	8.770	67.502	2.656	13.281	61.920
5	1.410	7.049	74.551	1.410	7.049	74.551	2.526	12.630	74.551
6	.917	4.583	79.134						
7	.826	4.128	83.262						
8	.526	2.628	85.890						
9	.471	2.354	88.245						
10	.413	2.067	90.312						
11	.392	1.960	92.272						
12	.324	1.621	93.893						
13	.274	1.372	95.265						
14	.224	1.121	96.386						
15	.197	.987	97.372						
16	.156	.778	98.150						
17	.126	.629	98.779						
18	.112	.559	99.338						
19	.073	.364	99.702						
20	.060	.298	100.000						

Extraction Method: Principal Component Analysis.

Section 4. Initial analysis – Orthogonal-rotated component matrix before scale purification

	Component					
Item	1	2	3	4	5	***Communality***
ADV1	***.792***	.069	-.164	.202	-.008	.700
ADV2	***.477****	.062	***.559****	-.142	-.062	.568
ADV3	***.768***	-.049	.275	.072	-.017	.674
ADV4	***.780***	.203	-.049	.100	.040	.664
ADV5	***.716***	.087	.123	.071	.051	.543
ADV6	***.689***	.164	.261	.026	.229	.623
TOP1	.071	.135	***.838***	.113	-.012	.739
TOP2	.260	.160	***.746***	.241	.131	.725
TOP3	-.167	.250	***.705***	.254	.081	.658
TOP4	.130	.000	***.765***	.183	.268	.707
PRE1	-.008	***.659****	.197	.322	.372	.716
PRE2	.148	***.902***	.143	.143	.055	.879
PRE3	.115	***.907***	.111	.170	.140	.897
PRE4	.212	***.867***	.114	.194	.155	.872
SUP1	.082	.331	.195	***.831***	.099	.854
SUP2	.149	.166	.170	***.905***	.076	.904
SUP3	.203	.215	.232	***.818***	.227	.862
TEC1	.088	.089	.286	.145	***.819***	.789
TEC2	.074	.141	.098	.097	***.901***	.857
TEC3	.017	.193	-.064	.076	***.796****	.681
						Total
Rotation Sum of Squares (Eigenvalues)	3.321	3.265	3.141	2.656	2.526	14.909
% of variance explained	16.607	16.326	15.707	13.281	12.630	74.551

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

Rotation converged in 6 iterations.

Section 5. Initial analysis – Item elimination

An additional PCA is conducted after elimination of each item described below.

→ Items eliminated during PCA

Eliminated item	*Convergent validity (Small component loading)*
x	x
Eliminated item	*Discriminant validity (Cross-loader)*
ADV2	.559 & .477

→ Items eliminated during reliability analyses

Eliminated item	Internal consistency (See Appendix D)
PRE1	x
TEC3	x

Section 6. Assumptions before conducting the final PCA – Anti-image matrix after scale purification

	ADV1	ADV3	ADV4	ADV5	ADV6	TOP1	TOP2	TOP3	TOP4	PRE2	PRE3	PRE4	SUP1	SUP2	SUP3	TEC1	TEC2
ADV1	**.633**																
ADV3	-.026	**.795**															
ADV4	-.714	-.256	**.674**														
ADV5	-.236	-.256	.200	**.755**													
ADV6	.198	-.130	-.273	-.423	**.784**												
TOP1	.229	-.219	-.139	.126	.213	**.713**											
TOP2	-.062	-.007	.038	-.173	-.285	-.536	**.751**										
TOP3	.138	.183	-.094	.060	.091	-.054	-.319	**.834**									
TOP4	-.159	.042	.143	.018	-.182	-.256	-.135	-.241	**.857**								
PRE2	.143	-.062	-.112	-.185	.075	-.126	.220	-.142	-.109	**.805**							
PRE3	.012	.138	.034	.111	.066	.280	-.434	.164	.082	-.458	**.753**						
PRE4	-.154	.053	-.016	.002	-.218	-.231	.228	-.074	.119	-.396	-.484	**.790**					
SUP1	.117	-.256	-.007	.130	.147	.018	.063	-.180	-.071	.135	.046	-.374	**.750**				
SUP2	-.044	.177	-.084	-.025	.013	.094	-.236	.125	.132	-.221	.136	.179	-.570	**.713**			
SUP3	-.178	-.021	.180	-.115	-.121	-.080	.105	-.052	-.115	.125	-.243	.103	-.301	-.437	**.859**		
TEC1	-.093	-.126	.118	.137	.016	-.131	.088	-.042	-.235	.082	-.025	-.139	.358	-.371	.009	**.628**	
TEC2	.183	.093	-.170	-.093	-.042	.192	-.089	.069	.046	-.020	-.003	.046	-.309	.390	-.145	-.789	**.579**

Note(s): Individual KMO-measures of sampling adequacy are bold on the diagonal, partial correlations on the off-diagonal **(**ADV2, PRE1, and TEC3 eliminated)

Section 7. Final analysis – Results for the extraction of components after scale purification

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	6.226	36.621	36.621	6.226	36.621	36.621	3.143	18.491	18.491
2	2.383	14.015	50.636	2.383	14.015	50.636	2.889	16.992	35.483
3	1.908	11.223	61.860	1.908	11.223	61.860	2.776	16.328	51.810
4	1.422	8.363	70.223	1.422	8.363	70.223	2.564	15.081	66.891
5	1.344	7.908	78.130	1.344	7.908	78.130	1.911	11.239	78.130
6	.872	5.130	83.260						
7	.607	3.568	86.829						
8	.422	2.480	89.308						
9	.385	2.264	91.573						
10	.334	1.962	93.534						
11	.251	1.474	95.009						
12	.229	1.346	96.354						
13	.189	1.112	97.467						
14	.159	.933	98.400						
15	.119	.699	99.098						
16	.080	.469	99.567						
17	.074	.433	100.000						

Extraction Method: Principal Component Analysis.

Section 8. Final analysis – Applying an oblique rotation to compare results with the orthogonal-rotated solution

Pattern matrix (after elimination of ADV2, PRE1, and TEC3)

Items	Component					Communality
	1	2	3	4	5	
ADV1	-.240	***.794***	-.021	-.082	-.185	.700
ADV3	.142	***.744***	.133	-.005	-.069	.601
ADV4	-.094	***.788***	-.168	-.074	-.026	.681
ADV5	.079	***.745***	-.023	.048	.052	.584
ADV6	.213	***.698***	-.106	.181	.133	.667
TOP1	***.872***	.031	-.060	-.086	.013	.753
TOP2	***.763***	.232	-.030	.008	-.091	.777
TOP3	***.751***	-.222	-.151	-.050	-.142	.688
TOP4	***.729***	.089	.121	.251	-.057	.724
PRE2	.070	.033	***-.931***	-.027	.018	.891
PRE3	-.010	-.021	***-.915***	.070	-.040	.890
PRE4	.006	.075	***-.895***	.049	-.059	.911
SUP1	.043	-.062	-.154	-.004	***-.865***	.879
SUP2	.035	.037	.052	-.022	***-.951***	.896
SUP3	.054	.075	-.004	.153	***-.838***	.870
TEC1	.064	-.017	-.005	***.892***	-.074	.871
TEC2	-.110	-.013	-.076	***.952***	-.018	.898

Extraction Method: Principal Component Analysis. Rotation Method: Oblimin with Kaiser Normalization.

a. Rotation converged in 7 iterations.

Structure matrix (after elimination of ADV2, PRE1, and TEC3)

Items	Component				
	1	2	3	4	5
ADV1	-.073	***.791***	-.192	.023	-.282
ADV3	.251	***.754***	-.086	.137	-.235
ADV4	.057	***.804***	-.309	.064	-.230
ADV5	.199	***.757***	-.191	.176	-.169
ADV6	.357	***.751***	-.292	.338	-.186
TOP1	***.862***	.166	-.242	.176	-.276
TOP2	***.839***	.383	-.293	.289	-.404
TOP3	***.781***	-.044	-.321	.198	-.378
TOP4	***.805***	.232	-.145	.458	-.326
PRE2	.275	.236	***-.941***	.201	-.377
PRE3	.230	.193	***-.940***	.278	-.415
PRE4	.257	.290	***-.947***	.277	-.448
SUP1	.345	.180	-.495	.248	***-.925***
SUP2	.328	.251	-.339	.219	***-.945***
SUP3	.379	.305	-.402	.390	***-.913***
TEC1	.339	.148	-.245	***.927***	-.315
TEC2	.181	.136	-.267	***.940***	-.247

Extraction Method: Principal Component Analysis. Rotation Method: Oblimin with Kaiser Normalization.

Component correlation matrix

Component	1	2	3	4	5
1	**1.000**				
2	.159	**1.000**			
3	-.230	-.214	**1.000**		
4	.283	.153	-.223	**1.000**	
5	-.321	-.235	.399	-.249	**1.000**

Extraction Method: Principal Component Analysis.

Rotation Method: Oblimin with Kaiser Normalization.

Appendix D – SPSS output: Reliability analysis

Reflective construct 1 – Perceived relative advantage

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.834	.834	5

Item	Cronbach's Alpha if Item Deleted
ADV2	.799
ADV3	.806
ADV5	.789
ADV6	.806
ADV7	.800

Reflective construct 2 - Top management support

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.851	.854	4

Item	Cronbach's Alpha if Item Deleted
TOP1	.800
TOP2	.796
TOP3	.836
TOP4	.813

Reflective construct 3 - Buyer/Supplier pressure

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.921	.922	4

Item	Cronbach's Alpha if Item Deleted
PRE1	.943
PRE2	.885
PRE3	.868
PRE4	.890

→ **Buyer/Supplier pressure (After elimination of PRE1)**

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.943	.943	3

Item	Cronbach's Alpha if Item Deleted
PRE2	.921
PRE3	.920
PRE4	.908

Reflective construct 4 - External support

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.927	.928	3

Item	Cronbach's Alpha if Item Deleted
SUP1	.902
SUP2	.886
SUP3	.897

Reflective construct 5 - Technological uncertainty

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.846	.845	3

Item	Cronbach's Alpha if Item Deleted
TEC1	.764
TEC2	.679
TEC3	.883

→ Technological uncertainty (After elimination of TEC3)

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.883	.883	2

Item	Cronbach's Alpha if Item Deleted
TEC1	.
TEC2	.

Appendix E – SPSS output: Additional descriptive statistics

Section 1. Cyber threat awareness

Cyber threat	Frequency of respondents that heard of threat	Percentage	Rank
1. Virus	73	100.0%	1
2. Spamming	73	100.0%	1
3. Hacking	73	100.0%	1
4. Phishing	72	98.6%	4
5. Spyware	69	94.5%	5
6. Ransomware	69	94.5%	5
7. Online purchase/selling fraud	69	93.5%	5
8. Online banking fraud	69	93.5%	5
9. Cyber extortion	69	93.5%	5
10. Trojan horse	67	91.8%	10
11. Cyber espionage	64	87.7%	11
12. Worm	57	78.1%	12
13. Spoofing	42	60.3%	13
14. CEO-fraud	38	52.1%	14
15. (Distributed) Denial-of-Service attack	36	49.3%	15
16. Online advance-fee fraud (419-scam)	22	30.1%	16
17. Pharming	19	26.0%	17
18. Man-in-the-middle attack	16	21.9%	18

Section 2. Cyber threat information sources

Information source	Frequency of respondents that utilized information source about cyber threats	Percentage	Rank
1. IT supplier	42	57.5%	1
2. Internet (Google, online forum, specialist sites)	25	34.2%	2
3. Internal colleagues	25	34.2%	2
4. Newspaper	23	31.5%	4
5. Other entrepreneurs / competitors	21	28.8%	5
6. Social media	20	27.4%	5
7. Television	17	23.3%	7
8. Interest / industry association	11	15.1%	8
9. Friends / family	11	15.1%	8
10. (Cyber) insurer	8	11.0%	10
11. Cybersecurity consultancy firm	7	9.6%	11
12. Scientific publications	7	9.6%	11
13. Internet provider	6	8.2%	13
14. Dutch Data Protection Authority	6	8.2%	13
15. Radio	6	8.2%	13
16. Digital Trust Centre	5	6.8%	16
17. Fraud Helpdesk	5	6.8%	16
18. Dutch Chambers of Commerce	4	5.5%	18
19. Financial bank	3	4.1%	19
20. Police	3	4.1%	19
21. Books	2	2.7%	21
22. Local authority	1	1.4%	22

Section 3. Cyber risk perception (individual scenarios)

Cyber scenario	N	MEAN	SD	MIN	MAX	RANGE	SKEW	KURT
1. CEO-FRAUD	73	5.25	2.63	1.00	11.00	10.00	.049	-.988
2. RANSOMWARE & CYBER EXTORTION	73	5.11	2.11	1.00	10.00	9.00	.145	-.499
3. DDOS-ATTACK	73	5.84	2.46	1.00	10.00	9.00	-.216	-.980

Section 4. Firm cyber experience (individual scenarios)

Cyber scenario	Frequency of respondents that experienced scenario	Percentage	Rank
1. DDOS-ATTACK	10	13.7%	1
2. CEO-FRAUD	10	13.7%	1
3. RANSOMWARE & CYBER EXTORTION	5	6.8%	3
Firm experienced at least 1 cyber scenario	20	27.4%	n/a

Appendix F – SPSS output: Ordinal logistic regression analysis

Section 1. Model 1 (Only control variables)

- **Warnings**

There are 1 (5.6%) cells (i.e., dependent variable levels by observed combinations of predictor variable values) with zero frequencies.

- **Case Processing Summary**

ADOPTIE_INTENTION	No/Low	19	26.0%
	Moderate	34	46.6%
	High	20	27.4%
FIRM_INDUSTRY	All other industries	59	80.8%
	Information and communication	14	19.2%
FIRM_SIZE	Micro	30	41.1%
	Small	29	39.7%
	Medium	14	19.2%
Valid		73	100.0%
Missing		0	
Total		73	

- **Model Fitting Information**

Model	-2 Log Likelihood[a]	Chi-Square	df	Sig.
Intercept Only	34.940			
Final	28.890	6.050	3	.109

Link function: Logit.
a. The kernel of the log-likelihood function is displayed.

- **Goodness-of-Fit**

	Chi-Square	df	Sig.
Pearson	.953	7	.996
Deviance	1.380	7	.986

Link function: Logit.

- **Pseudo R-Square**

Cox and Snell	.080
Nagelkerke	.090
McFadden	.039

Link function: Logit.

- **Parameter Estimates**

						95% Confidence Interval	
		Estimate	Std. Error	Wald	df	Sig.	Lower Bound	Upper Bound
Threshold	[ADOPTION_3 = 1,00]	-.434	.369	1.386	1	.239	-1.156	.288
	[ADOPTION_3 = 2,00]	1.728	.428	16.277	1	<.001	.889	2.568
Location	[FIRM_SIZE=micro]	0[a]	.	.	0	.	.	.
	[FIRM_SIZE=small]	1.085	.507	4.574	1	.032	.091	2.079
	[FIRM_SIZE=medium]	1.184	.626	3.578	1	.059	-.043	2.411
	[FIRM_INDUSTRY= all other industries]	0[a]	.	.	0	.	.	.
	[FIRM_INDUSTRY= info. & comm.]	.086	.562	.023	1	.878	-1.015	1.187

- **Test of Parallel Lines[a]**

Model	-2 Log Likelihood[b]	Chi-Square	df	Sig.
Null Hypothesis	28.890			
General	28.645	.245	3	.970

The null hypothesis states that the location parameters (slope coefficients) are the same across response categories.
a. Link function: Logit.
b. The kernel of the log-likelihood function is displayed.

Section 2. Model 2 (Independent variables + control variables)

- **Warnings**

There are 156 (66.7%) cells (i.e., dependent variable levels by observed combinations of predictor variable values) with zero frequencies.

- **Case Processing Summary**

		N	Marginal Percentage
ADOPTIE_INTENTION	No/Low	19	26.0%
	Moderate	34	46.6%
	High	20	27.4%
FIRM_INDUSTRY	All other industries	59	80.8%
	Information and communication	14	19.2%
FIRM_SIZE	Micro	30	41.1%
	Small	29	39.7%
	Medium	14	19.2%
Valid		73	100.0%
Missing		0	
Total		73	

- **Model Fitting Information**

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	154.897			
Final	111.057	43.840	10	<.001

Link function: Logit.

- **Goodness-of-Fit**

	Chi-Square	df	Sig.
Pearson	139.416	134	.357
Deviance	111.057	134	.926

Link function: Logit.

- **Pseudo R-Square**

Cox and Snell	.451
Nagelkerke	.513
McFadden	.283

Link function: Logit.

- **Parameter Estimates**

		Estimate	Std. Error	Wald	df	Sig.	95% Confidence Interval	
							Lower Bound	Upper Bound
Threshold	[CIRP_ADOPTION = 1,00]	8.026	1.976	16.501	1	<.001	4.153	11.898
	[CIRP_ADOPTION = 2,00]	11.331	2.272	24.866	1	<.001	6.877	15.784
Location	RELATIVE_ADVANTAGE	.420	.298	1.985	1	.159	-.164	1.004
	MANAGEMENT_SUPPORT	.978	.310	9.946	1	.002	.370	1.586
	RESOURCE_AVAILABILITY	.207	.268	.596	1	.440	-.318	.731
	BUYER_SUPPLIER_PRESSURE	.391	.228	2.948	1	.086	-.055	.837
	EXTERNAL_SUPPORT	-.194	.250	.602	1	.438	-.685	.296
	TECHNOLOGICAL_UNCERTAINTY	-.279	.203	1.884	1	.170	-.677	.119
	CYBER_RISK_PERCEPTION	.506	.174	8.458	1	.004	.165	.846
	[FIRM_SIZE=micro]	0[a]	.	.	0	.	.	.
	[FIRM_SIZE=small]	.326	.586	.311	1	.577	-.821	1.474
	[FIRM_SIZE=medium]	.563	.731	.595	1	.441	-.869	1.996
	[FIRM_INDUSTRY=all other industries]	0[a]	.	.	0	.	.	.
	[FIRM_INDUSTRY=info. & comm.]	.741	.757	.958	1	.328	-.743	2.225

Link function: Logit.
a. This parameter is set to zero because it is redundant.

- **Test of Parallel Lines[a]**

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Null Hypothesis	111.057			
General	105.641	5.416	10	.862

The null hypothesis states that the location parameters (slope coefficients) are the same across response categories.
a. Link function: Logit.