Master Thesis

Cybercrime and Cybersecurity in the Dutch Retail Sector: A Nationwide Analysis

A.N.J.P.M. (Alexander) Haas

Main supervisor: prof. dr. M. (Marianne) Junger
Secondary supervisor: dr. A. (Abhishta) Abhishta

MSc Business Administration
University of Twente – 18 July 2021

Acknowledgements I would like to thank and acknowledge my main supervisor, prof. dr. Marianne Junger, for her valuable and encouraging feedback on earlier versions of this work. I feel very fortunate to have benefited from her vast expertise in the course of the past eight months. I would also like to thank my secondary supervisor, dr. Abhishta Abhishta, for all of his valuable help during the final stages of this project. My younger brother Christiaan deserves credit for proofreading the final version of this text. Finally, I would like to express my sincere gratitude to the hundreds of individuals who sacrificed some of their time to participate in this study.

Abstract This study had three aims. First of all, it aimed to establish how prevalent cybercrime is among small and medium-sized retail stores in the Netherlands. Secondly, it aimed to establish to what extent such stores are taking basic cybersecurity measures to protect themselves against cybercrime. Finally, it aimed to explain why some small and medium-sized Dutch retail stores are taking more basic cybersecurity measures than others. A survey was developed on the basis of an extensive literature review. Approximately 3500 stores from all over the Netherlands were invited to participate in that survey. Useful data was collected for 351 businesses. It was found that cybercrime is not as prevalent among small and medium-sized Dutch retail stores as previous research would suggest. At the same time, however, many Dutch retail stores appear to be unnecessarily vulnerable to cybercrime because they are failing to take some basic cybersecurity measures. Several factors were identified that may play a role in retail stores' decision-making about basic cybersecurity measures. The practical implications of these findings will be discussed and suggestions for future work will be provided.

Table of Contents

1. Introduction

In the course of the past five decades, enormous advancements have been made in the areas of computer science and electrical engineering. In many respects, this technological progress has changed the way people live their lives (Moitra, 2005, p. 105; Holt & Bossler, 2014, p. 20; Odinot et al., 2017, p. 11; Saleem et al., 2017, p. 1; Bada & Nurse, 2019, p. 2). They look up information online nowadays instead of consulting printed encyclopaedias, for example, and they navigate the world with the help of their smartphones instead of relying on hardcopy maps. Roughly half of the world's population regularly accesses the Internet, according to one recent estimate (International Telecommunication Union, 2020, p. 7). Europe appears to be a front-runner in this area (International Telecommunication Union, 2020, p. 7). The Netherlands, in turn, boasts a higher Internet adoption rate than any other country in the European Union: approximately 98% of all Dutch households have access to the Internet (Statistics Netherlands, 2019b, p. 71). The same is true for virtually all Dutch companies, many of which are highly digitalised (Veenstra et al., 2015, p. 13+20; Odinot et al., 2017, p. 11; Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2020, p. 7).

Without doubt, the rise of modern technology has brought mankind many benefits. People have greater access to information than ever before, for example, and communicating with others across vast distances has never been as easy (or cheap) as it is today. Unfortunately, there is also another side to the coin. In this digitalised society, both individuals and organisations are constantly at risk of falling victim to cybercrime (Moitra, 2005, p. 105; Misra et al., 2017, p. 1; Odinot et al., 2017, p. 11; Saleem et al., 2017, p. 1; Reep-Van den Bergh & Junger, 2018, p. 1; Martens et al., 2019, p. 139). Many scholars seem to agree that this is a serious cause for concern (Holt & Bossler, 2014, p. 21; Riek et al., 2015, p. 261; Van de Weijer & Leukfeldt, 2017, p. 407; Akhgar et al., 2019, p. 196; Anderson et al., 2019, p. 5; Martens et al., 2019, p. 139; Van de Weijer et al., 2019, p. 486; Wanamaker, 2019, p. 3; Cheng et al., 2020, p. 1; Norris & Brookes, 2021, p. 1).

Individuals and organisations can reduce the probability that they will fall victim to cybercrime by taking a number of basic cybersecurity measures. They would be well-advised to use reliable antivirus software, for instance, and to protect all of their devices with a strong password. Although such basic cybersecurity measures tend to be simple and cheap to implement, there is reason to believe than many individuals and organisations are failing to do so. In the academic literature, there have been calls for more research on why this is the case (Crossler, 2010, p. 1; Hanus & Wu, 2016, p. 3; Martens et al., 2019, p. 139). Individuals and organisations should be encouraged to enhance their digital resilience. Not much is known yet about how this can be done in an effective manner, however (Bada & Nurse, 2019, p. 5; Jansen & Van Schaik, 2019, p. 40).

This study investigated cybercrime and cybersecurity at retail stores. It had three aims. First of all, it aimed to establish how prevalent cybercrime is among small and medium-sized retail stores in the Netherlands. Secondly, it aimed to establish to what extent such stores are taking basic cybersecurity measures to protect themselves against cybercrime. Finally, it aimed to explain why some small and medium-sized Dutch retail stores are taking more basic cybersecurity measures than others.

The Dutch retail sector employs circa 800.000 people and makes "major contributions to the Dutch economy" (Kuijpers et al., 2016, p. 12). Hence, it seems important for the businesses in that sector to protect themselves against cybercrime. Almost all Dutch retail stores (99%) have fewer than 50 employees (Kuijpers et al., 2016, p. 10). A study on cybercrime and cybersecurity at small and medium-sized retail stores in The Hague recently found that half of all participating stores had fallen victim to cybercrime in the preceding year (Van der Kleij et al., 2019). It needs to be examined whether this finding can be replicated at a national level. If so, many small and medium-sized Dutch retail stores should probably start to take more basic cybersecurity measures. To develop an effective campaign to encourage them to do so, it could be valuable to know which factors and considerations are preventing them from taking their cybersecurity more seriously already at this moment.

The remainder of this thesis will be structured as follows. In section 2, a brief overview of the academic literature on cybercrime will be provided. In section 3, existing statistics about cybersecurity and cybercrime at Dutch SMEs will be discussed. The aims and relevance of the present study will be elaborated upon in section 4. This will be followed by a detailed description of the set-up of this study in section 5. In sections 6 and 7, the results of this study will be presented and discussed, respectively. A summary and some concluding remarks will be provided in section 8.

2. Academic background

2.1. Defining cybercrime

There exist many different types of cybercrime. Think of illegally hacking into someone else's computer, for example, or of scamming someone via the Internet (Bauer & Van Eeten, 2009, p. 707; Leukfeldt & Yar, 2016, p. 263; Martens et al., 2019, p. 139-140; Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2020, p. 7; Politie Nederland, n.d.). Some types of cybercrime, like phishing, can best be seen as modern versions of traditional (offline) criminal activities (Misra et al., 2017 p. 2). Other types of cybercrime, like spreading malware or committing a DDoS attack, do not have obvious offline counterparts and can therefore be deemed truly "new and distinctive" (Yar, 2005, p. 423). Some scholars like to refer to the former types of cybercrime as 'computer-assisted' ones, and to the latter as 'computer-focused' ones (Furnell, 2001, p. 31; Yar, 2005, p. 409). Similar distinctions have been made by others in the past (European Commission, 2007, p. 2; Paoli et al., 2017, p. 3; Buil-Gil et al., 2020, p. 2).

The term 'cybercrime', in sum, covers a "broad range of different criminal activities" that involve "computers and information systems" (European Commission, 2013, p. 3; Reep-Van den Bergh & Junger, 2018, p. 2). Combined with the fact that the *modi operandi* of cybercriminals tend to evolve at a very rapid pace (Rechtman, 2017; Reep-Van den Bergh & Junger, 2018, p. 1+12; Carías et al., 2020, p. 174200; Statistics Netherlands, n.d.), this makes it difficult to develop a comprehensive definition of the term in question. Academics have not refrained from attempting to do so, however. On the contrary: many different definitions of cybercrime can be found in the literature (Fafinski et al., 2010, p. 4; Ngo & Paternoster, 2011, p. 773; Holt & Bossler, 2014, p. 21). One group of researchers once aptly referred to this diversity as a "definitional cacophony" (Paoli et al., 2017, p. 3).

Different scholars have different views on the extent to which modern technology should be involved in a criminal activity in order for it to qualify as a cybercrime. Some scholars seem to believe that cybercrimes do not necessarily have to rely very heavily on computers (Ngo & Paternoster, 2011, p. 773). Others, however, seem to believe that a significant involvement of computers is a *sine qua* *non* without which a criminal activity cannot be called a cybercrime (Yar, 2005, p. 409). Adherents of this view believe that the term 'cybercrime' should not be diluted too much, fearing that an overly flexible definition would render it useless. Arguably, as one scholar already noted more than three decades ago, it would be inconvenient if the definition of cybercrime would be expanded to include offenses like destroying someone else's computer with a baseball bat (Ingraham, 1980, p. 438). Some academics believe a criminal activity should only be called a cybercrime if "a computer (…) is the instrument of the crime *and* a computer (…) is the target of the crime" (Moitra, 2004, p. 106).

For the purposes of this thesis, the term 'cybercrime' will be defined to include all criminal activities that are committed by means of modern technology. Others have adopted similar definitions in the past (Ngo & Paternoster, 2011, p. 773; Veenstra et al., 2015, p. 4; Rechtman, 2017; Statistics Netherlands, 2019a, p. 27). This paper's working definition does not cover harmful cyberactivities that are legal, like online bullying, however undesirable they may be (Fafinski et al., 2010, p. 5).

2.2. Academic interest in cybercrime

Researchers appear to be growing increasingly interested in cybercrime. Each year, more articles get published on cybercrime than the year before. Please see figure 1, which was made with data from the Scopus database (search term: 'cybercrime'). Cybercrime can be studied from many different angles and has attracted the attention of many different types of scholars, ranging from computer scientists to jurists and from economists to electrical engineers (Paoli et al., 2017, p. 3). Surprisingly, perhaps, it seems that cybercrime initially did not receive much attention from criminologists (Jaishankar, 2018, p. 1). Fortunately, that has changed in the course of the past three decades (Holt & Bossler, 2008, p. 2; Bossler & Holt, 2010, p. 227; Nhan & Bachmann, 2010, p.

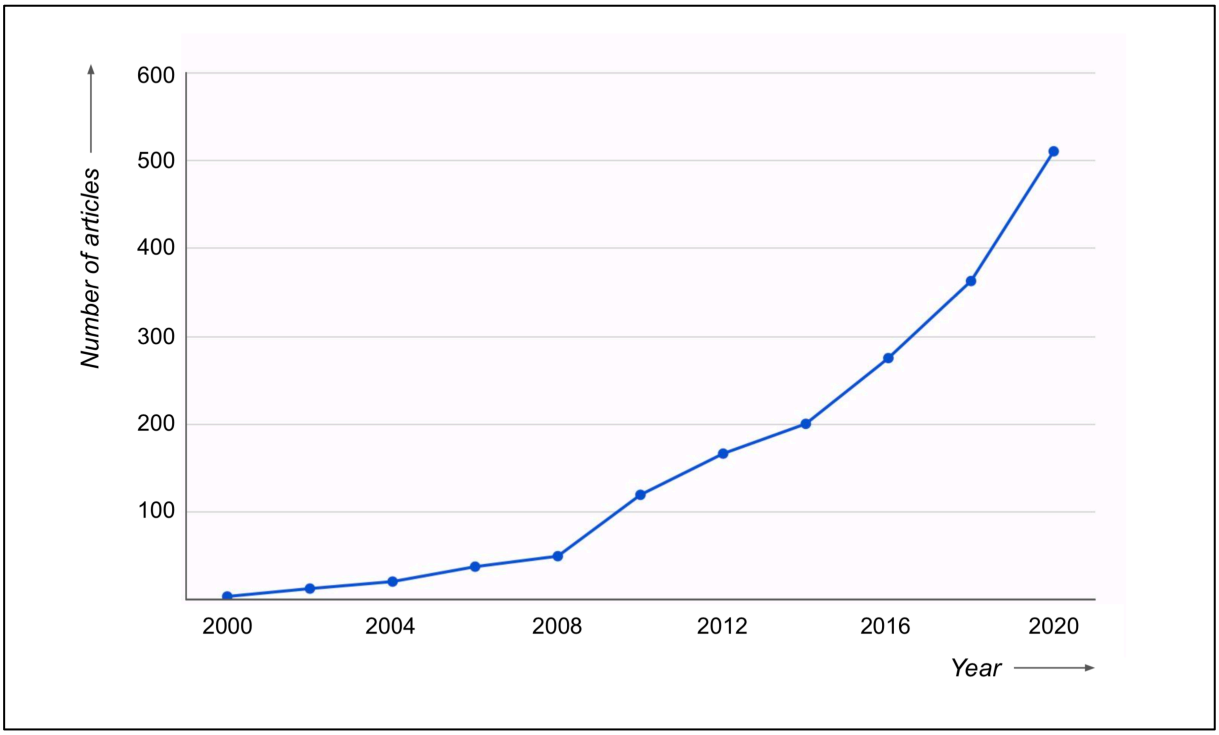

Figure 1. More articles seem to get published on cybercrime each year. Research in this area is truly booming.

175; Ngo & Paternoster, 2011, p. 773; Holt & Bossler, 2014, p. 20-21+33; Jaishankar, 2018, p. 6). The study of cybercrime is now an "established area of criminological research" (Leukfeldt & Yar, 2016, p. 263). Indeed, the criminological study of cybercrime seems to be booming at the moment.

2.3. More research is needed

Although a substantial amount of cybercrime-focused research has already been conducted, it could be argued that "cybercrime as a subject of study is still in its infancy" (Armin et al., 2015, p. 20). The criminological study of cybercrime has a relatively brief history (Cheng et al., 2020, p. 7), which should not be surprising given the fact that cybercrime itself is a relatively new phenomenon. To develop a better understanding of this phenomenon and how to tackle it, more research is needed (Holt & Bossler, 2014, p. 33; Odinot et al., 2017, p. 7). There have been calls for more research that focuses on identifying causes and correlates of cybercrime victimisation, for example (Bossler & Holt, 2010, p. 227; Ngo & Paternoster, 2011, p. 774; Cheng et al., 2020, p. 2). It should be noted that some interesting work was already conducted in this area recently (Reyns & Henson, 2015; Junger et al., 2017; Reep-Van den Bergh & Junger, 2018; Weulen Kranenbarg et al., 2019). There have also been calls for more research on why many individuals and organisations fail to protect themselves against cybercrime (Crossler, 2010, p. 1; Hanus & Wu, 2016, p. 3; Martens et al., 2019, p. 139). It is believed that more knowledge in this area could be leveraged to effectively encourage poorly-protected individuals and organisations to enhance their digital resilience (Bockarjova & Steg, 2014, p. 277). Not much is known yet about how to successfully motivate people to behave in a cybersecure manner (Bada & Nurse, 2019, p. 5). Indeed, as one pair of scholars recently put it, work in this area is "just getting started" (Jansen & Van Schaik, 2019, p. 40).

3. Cybercrime and cybersecurity at Dutch SMEs

3.1. A critical note on cyberstatistics

Before we examine some existing statistics about cybercrime and cybersecurity at Dutch SMEs, it should be noted that such statistics often need to be treated with caution. Government statistics tend to be incomplete, and statistics published by commercial parties may not always be reliable.

3.1.1. Official government statistics

Even for government agencies, collecting accurate cybercrime statistics can be "extremely difficult" (Moitra, 2004, p. 108; Armin et al., 2015, p. 2; Riek et al., 2015, p. 261; Anderson et al., 2019, p. 2). One complicating factor is the fact that many cybercrime victims do not report their victimhood to the police. Cybercrime underreporting can be observed all over the world (Fafinski et al., 2010, p. 4+12+13; Wanamaker, 2019, p. 1+3), including in the Netherlands (Veenstra et al., 2015, p. 10; Van de Weijer et al., 2019, p. 486). A Canadian study recently found that only half of all companies that fall victim to cybercrime contact the official authorities, for example (Wanamaker, 2019, p. 1). Similar reporting rates have been observed in the United Kingdom (Armin et al., 2015, p. 4; Buil-Gil et al., 2020, p. 10). Companies may refrain from contacting the police for various reasons. They may fear reputational damage, for example, or they may believe that the authorities will not be able to help them anyway (Fafinski et al., 2010, p. 2; Veenstra et al., 2015, p. 10; Renaud & Weir, 2016, p. 141; Van de Weijer et al., 2019; Wanamaker, 2019, p. 6). Unfortunately, the latter belief may be justified. It is "extremely difficult to investigate and prosecute cybercrime" (Boes & Leukfeldt, 2017, p. 186; Odinot et al., 2017, p. 11), partly as a result of the borderless nature of the Internet. This is reflected in the official police statistics. In 2015, for example, the Dutch police identified suspects in only 4.6% of all cybercrime cases that were reported to them that year (Centraal Planbureau, 2018, p. 2). Not surprisingly, cybercriminals do not seem to be very worried about getting punished for their actions (Zhang et al., 2007, p. 34).

Even if cybercrime incidents do get reported to the police, they may not always end up in official cybercrime statistics. In the Netherlands, for example, reported incidents may be excluded from the statistics if no official charges are pressed (Veenstra et al., 2015, p. 11). Charges are pressed in only 8% of all cybercrime cases in the Netherlands (Statistics Netherlands, 2019c, p. 9). Reported incidents may also be excluded from the official statistics if the police officers who are involved in registering them lack certain basic knowledge about cybercrime (Boes & Leukfeldt, 2017, p. 189).

Statistics Netherlands, the statistics agency of the Dutch government, acknowledges that the figures it publishes on cybercrime are incomplete and that "the magnitude of cybercrime" in the Netherlands "is currently unknown" (Statistics Netherlands, n.d.). This is regrettable. Without accurate statistics, it is difficult to evaluate whether new measures should be taken (or whether past measures have had any effect) (Fafinski et al., 2010, p. 2; Armin et al., 2015, p. 20). As Statistics Netherlands recently concluded, collecting "better information" on cybercrime and cybersecurity is "crucial" (Centraal Planbureau, 2019a). The present study aimed to make a modest contribution in this area.

3.1.2. Statistics published by commercial parties

Apart from official government statistics, plenty of other statistics on cybercrime can also be found online and in the literature. Many of those statistics can be traced back to reports published by companies in the cybersecurity industry. The reports in question tend to be quite shocking to read. McAfee, for example, recently claimed that cybercrime costs the world more than US$1 trillion each year (Smith & Lostri, 2020, p. 3). In 2020, Cybersecurity Ventures even estimated that figure to be upward of US$6 trillion (Morgan, 2020). Deloitte recently stated that cybercrime costs the Dutch economy €10 billion each year (De Groot, 2017). Likewise, KPN recently claimed that the average financial damage caused by a cyberattack exceeds €125,000 for Dutch companies (KPN, 2020).

It would go too far to accuse cybersecurity companies of making up shocking figures to attract more customers (Fafinski et al., 2010, p. 14), but it is important to note that such companies have "a particular view on the world" and "a specific agenda" (Anderson et al., 2019, p. 2). The figures that they publish should be treated with caution, therefore. Many others have already pointed this out in the past (Moitra, 2004, p. 109; Fafinski et al., 2010, p. 4; Maass & Rajagopalan, 2012; Armin et al., 2015, p. 2; Riek et al., 2015, p. 265; Gañán et al., 2017, p. 3; Paoli et al., 2017, p. 11). In spite of this, worryingly, questionable statistics are still regularly cited (uncritically) in articles and reports of an academic nature (Wiederhold, 2014, p. 131; Renaud & Weir, 2016, p. 137; Van Bavel et al., 2019, p. 29; Wanamaker, 2019, p. 3; Wang, 2019, p. 1; Benz & Chatterjee, 2020, p. 531).

3.1.3. Statistics that will be included here

In this thesis, cyberstatistics that have been published by parties with commercial interests will be avoided as much as possible. Official government statistics will be included, however, despite their shortcomings. A major strength of such statistics is that they can be trusted to have been compiled in an objective and impartial manner. The same is true for statistics that are the result of academic research. Such statistics will also be included in this thesis. It should be noted that they may also suffer from shortcomings, though, for instance as a result of limited sample sizes. Besides, "very few" academic studies on cybercrime and cybersecurity at SMEs seem to have been conducted so far (Valli et al., 2013, p. 1). The first major Dutch study in this area was only published in 2015 (Veenstra et al., 2015, p. 4). Before then, according to the authors of the study in question, cybercrime at Dutch SMEs had "barely been investigated" at all (Veenstra et al., 2015, p. 5).

3.2. Cybercrime prevalence

It is often claimed that small and medium-sized enterprises are primary targets for cybercriminals (Hayes & Bodhani, 2013, p. 80; Kurpjuhn, 2015, p. 5; Mijnhardt et al., 2016, p. 106; Renaud & Weir, 2016, p. 137; Carías et al., 2020, p. 174200; KPN, 2020; Lloyd, 2020, p. 15; Ponsard & Grandclaudon, 2020, p. 336). The Dutch domain name organisation, for example, recently stated that "SMEs form an easy and interesting target" for cybercriminals and that it is "a stubborn misconception that large businesses are the main targets of cybercrime" (Stichting Internet Domeinregistratie Nederland, 2020, p. 4). Such statements are remarkable, since official Dutch government statistics point in a different direction. Those statistics seem to suggest that large businesses are more likely to be targeted by cybercriminals than their smaller counterparts (Statistics Netherlands, 2019a, p. 19-20). Roughly 66% of all Dutch companies with more than 500 employees experienced a cybercrime incident in 2017, for example, whereas the same was true for only 18% of all Dutch companies that employed at most two people at the time (Statistics Netherlands, 2019a, p. 19-20). Other research also seems to suggest that large companies are targeted more often by cybercriminals than small companies, both in the Netherlands (MKB Nederland, 2017; Junger et al., 2020, p. 9) and abroad (Wanamaker, 2019, p. 6+8; Verizon, 2020, p. 7-8).

Large companies may be more attractive targets because they tend to have more financial resources (Statistics Netherlands, 2019a, p. 20). In addition, they tend to be relatively visible to the general public. This may play a role as well (Statistics Netherlands, 2019a, p. 20; Verizon, 2020, p. 8).

Although SMEs do not seem to be targeted as often by cybercriminals as their larger siblings, the threat that cybercrime poses to them is far from trivial. Research suggests that each year roughly 20% of all small and medium-sized enterprises in the Netherlands experience a cybercrime incident (Veenstra et al., 2015, p. 8+9; MKB Nederland, 2017; Notté & Slot, 2017, p. 1; Centraal Planbureau, 2018, p. 2; Statistics Netherlands, 2019a, p. 19-20; Stichting Internet Domeinregistratie Nederland, 2020, p. 4). Moreover, some scholars believe that the number of cybercrime incidents at SMEs is on the rise (Hayes & Bodhani, 2013, p. 80; Renaud, 2016, p. 10; Renaud & Weir, 2016, p. 137; Bada & Nurse, 2019, p. 2). Statistics Netherlands has not observed such a trend yet (Statistics Netherlands, 2021a, p. 22), but the results of a recent Dutch study do seem to confirm its existence (Stichting Internet Domeinregistratie Nederland, 2020, p. 4).

3.3. Cybersecurity behaviour

Given the threat that cybercrime poses to them, it seems small and medium-sized companies in the Netherlands would be well-advised to take their cybersecurity seriously. Unfortunately, many of the companies in question seem to be poorly protected against cybercrime (Centrum voor

Criminaliteitspreventie en Veiligheid, 2020). Official government statistics suggest that small Dutch businesses take fewer cybersecurity measures than their larger counterparts (Centraal Planbureau, 2018, p. 2+16; Statistics Netherlands, 2019a, p. 7+9). The employees of such companies also tend to be more concerned about their workplace's cybersecurity than the employees of larger businesses (Hengstz & Van der Grient, 2020, p. 6-7). Similar patterns can be observed in other countries (Renaud, 2016; Renaud & Weir, 2016, p. 137): all over the world, SMEs seem to form the "least mature and most vulnerable" of all business groups (Benz & Chatterjee, 2020, p. 531; Hayes & Bodhani, 2013, p. 81; Kurpjuhn, 2015, p. 6; Ponsard & Grandclaudon, 2020, p. 340).

According to the Dutch Bureau for Economic Policy Analysis, it is not entirely clear what causes the lack of cybersecurity measures among Dutch SMEs (Centraal Planbureau, 2018, p. 18). Research suggests that small and medium-sized companies tend to suffer from a lack of resources and knowledge, however, which can make it hard for them to "acknowledge threats and make themselves resilient" (Stichting Internet Domeinregistratie Nederland, 2020, p. 4; Osborn, 2014, p. 12). Many scholars seem to share this view (Valli et al., 2013, p. 1; Verbano & Venturini, 2013, p. 187; Brustbauer, 2016, p. 70; Mijnhardt et al., 2016, p. 106; Renaud & Weir, 2016, p. 139; Saleem et al., 2017, p. 1; Akhgar et al., 2019, p. 207; Bada & Nurse, 2019, p. 2; Bekkers et al., 2020, p. 2; Benz & Chatterjee, 2020, p. 532; Carías et al., 2020, p. 174201+174202; Ponsard & Grandclaudon, 2020, p. 338-340). When one's resources are limited, it may not be attractive to invest in cybersecurity. The immediate costs of such investments are very concrete, after all, whereas its long-term benefits are both abstract and uncertain (West, 2008; Kurpjuhn, 2015, p. 5; Renaud, 2016, p. 12). Many SMEs also seem to think that they are protected by their size, (mistakenly) believing that cybercriminals are only interested in attacking large organisations with deep pockets (Saleem et al., 2017, p. 1; Centraal Beheer, 2019, p. 2; Van der Kleij et al., 2019; Benz & Chatterjee, 2020, p. 532; Ponsard & Grandclaudon, 2020, p. 339).

As a result of their seemingly poor digital resilience, Dutch SMEs are running unnecessary risks (Centraal Planbureau, 2018, p. 16). It would be desirable for them to take more measures to protect themselves against cybercrime (Hayes & Bodhani, 2013, p. 80; Osborn, 2014, p. 1; Renaud, 2016, p. 11; Benz & Chatterjee, 2020, p. 532+538; Carías et al., 2020, p. 174200; Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2020, p. 7). Dutch SMEs tend to be strongly digitalised (Veenstra et al., 2015, p. 7), so a successful cyberattack could potentially cause them great damage (Valli et al., 2013, p. 1; Veenstra et al., 2015, p. 9-10; Renaud, 2016, p. 11; Van der Kleij et al., 2019). Besides, poorly-protected SMEs could be used as "attack vectors" by cybercriminals to victimise other parties (such as customers and supply chain partners) as well (Hayes & Bodhani, 2013, p. 82; Osborn, 2014, p. 4; Twisdale, 2018; Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2020, p. 7). This approach, in which small and weak targets are used as stepping stones towards larger (or more) fish, appears to be growing increasingly popular among cybercriminals (Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2020, p. 15).

Just like there exist many different types of cybercrime, there also exist many different types of cybersecurity measures. Some of those measures are very complex cannot be expected to be implemented by small and medium-sized enterprises – even the Dutch government appears to be struggling with them (Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2020, p. 8). Other cybersecurity measures, which will be referred to as 'basic' hereinafter, are much more accessible. Basic cybersecurity measures are cheap and easy to implement. Some of them, like using reliable antivirus software, reduce the likelihood that one will fall victim to cybercrime. Others, like regularly making back-ups of one's most important data, reduce the likelihood that falling victim to cybercrime will have a major impact. There exist many different basic cybersecurity measures (Kurpjuhn, 2015, p. 7; Renaud, 2016, p. 11; Saleem et al., 2017, p. 4-5; Carías et al., 2020, p. 174201; Lloyd, 2020, p. 17). Although such measures are unlikely to offer companies much protection against dedicated cybercriminals, they are believed to be effective against run-of-the-mill attacks (which are most common) (Herjavec, 2019, p. 9; Leukfeldt & Yar, 2016, p. 270). One could compare taking basic cybersecurity measures with locking up one's windows at night: professional criminals might still be able to sneak inside, but petty thieves will probably decide to try their luck elsewhere. The more cyber-security measures a company takes, the less worried it needs to be about cybercrime (Statistics Netherlands, 2019a, p. 9; Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2020, p. 8).

4. The present study

The aim of this study was to investigate cybercrime and cybersecurity at small and medium-sized retail stores in the Netherlands. How prevalent is cybercrime among such retail stores? To what extent are they taking basic cybersecurity measures to enhance their digital resilience? And how can we explain the fact that some small and medium-sized Dutch retail stores seem to be taking their cybersecurity more seriously than others? These questions formed the foundation of this study.

4.1. The Dutch retail sector

The Dutch retail sector consists of approximately 90.000 stores (Detailhandel Nederland, 2019). Virtually all of those stores have fewer than 50 employees (Kuijpers et al., 2016, p. 10). Those stores will be referred to as small and medium-sized retail stores in this thesis. In total, the Dutch retail sector employs circa 800.000 people (Detailhandel Nederland, 2019, p. 9). Given their importance to the Dutch economy (Kuijpers et al., 2016, p. 12), it seems relevant to study whether small and medium-sized Dutch retail stores fall victim to cybercrime often and whether they are taking basic cybersecurity measures to enhance their digital resilience.

Many Dutch retail stores appear to be growing increasingly dependent on modern technology (Detailhandel Nederland, 2018; Detailhandel Nederland, 2019, p. 14). As figure 2 on the next page shows, online sales are becoming a major source of revenue for the Dutch retail sector (Detailhandel Nederland, 2019, p. 9; Statistics Netherlands, 2021b; Bureau RMC, n.d.). As a consequence, retail stores are becoming increasingly vulnerable to cybercrime (Van der Kleij et al., 2019; Verizon, 2020, p. 73). According to some, they already form attractive targets for cybercriminals at this moment (Hayes & Bodhani, 2013, p. 81, Van der Kleij et al., 2019; Verizon, 2020, p. 73; Laane et al., 2021, p. 8). This can perhaps be explained by their large cash flows (Alshalan, 2006, p. 29), their high visibility (Leukfeldt & Yar, 2016, p. 279), or their possession of valuable customer data (Alshalan, 2006, p. 28; Verizon, 2020, p. 73; Laane et al., 2021, p. 23).

4.2. Existing research in this area

Only two studies appear to have investigated cybercrime and cybersecurity in the Dutch retail sector before. In 2018, a (now defunct) branch organisation commissioned a study on this topic (Cybercrime Info, 2018; Detailhandel Nederland, 2018). The study in question boasted a large

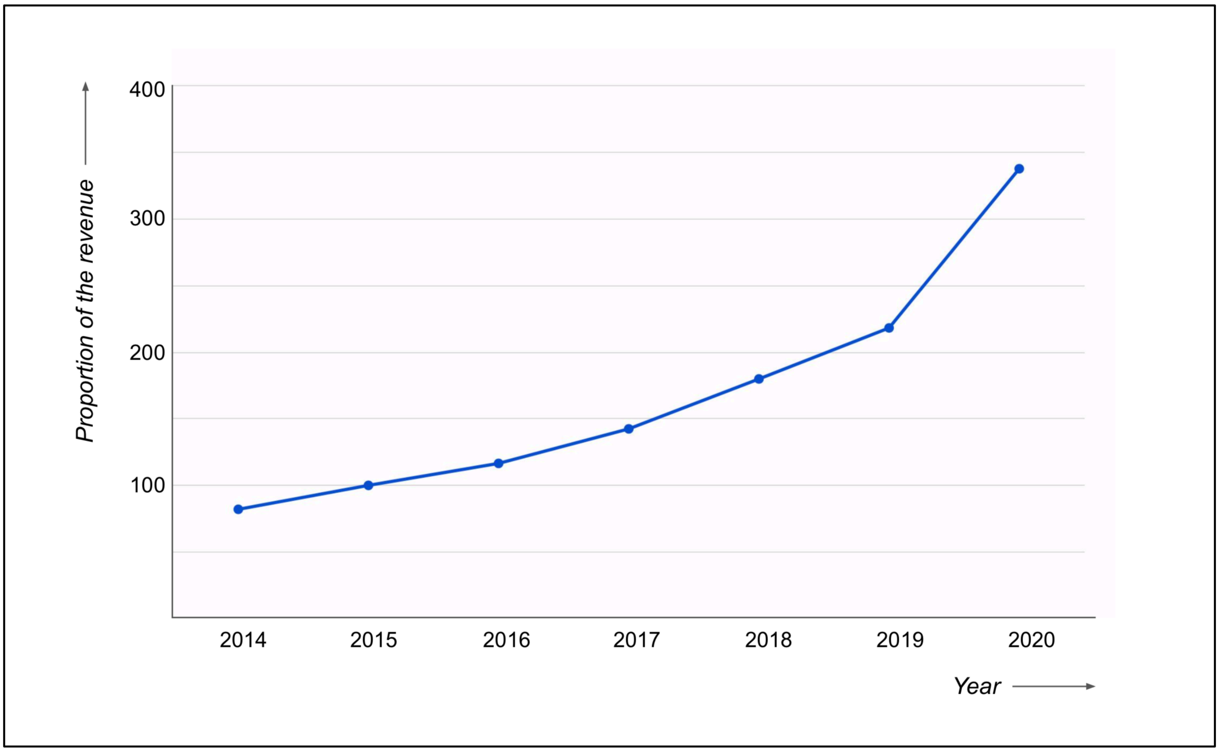

Figure 2. Online sales are becoming increasingly important for Dutch retail stores. Benchmark (100%): 2015.

- -

number of participants, but it did not focus exclusively on small and medium-sized stores. Moreover, its findings may no longer be valid today. The study also was not reported on in an academic journal, merely in a professional journal. This makes it hard to evaluate its scientific value. In 2019, another group of researchers investigated cybercrime and cybersecurity at small and medium-sized retail stores in The Hague (Van der Kleij et al., 2019). Only a small number of stores participated in that study, and it is unclear whether its results can be generalised to the Netherlands as a whole. Besides, this study was not reported on in an academic journal either.

What were the outcomes of these past research efforts? The 2018 study found that approximately 13% of all participating retail stores had experienced a cybercrime incident at least once in the course of their existence (Detailhandel Nederland, 2018). The most encountered types of cybercrime were phishing (47%), ransomware (28%) and hacking (23%). The study also found that many retail stores were “not aware of the threat that is posed by cybercrime” and failed to take basic cybersecurity measures (Detailhandel Nederland, 2018). Only 43% of all respondents made use of antivirus software, for example, and only 40% of them had protected their Wi-Fi networks with a password. The 2019 study, which focused exclusively on small and medium-sized retail stores in The Hague, painted an even more disturbing picture (Van der Kleij et al., 2019). It found that roughly half of all participating stores had experienced a cybercrime incident in the course of the preceding year, and that “SME retailers in and around The Hague are barely resilient against cybercrime” (Van der Kleij et al., 2019).

It is important to examine whether these results can be replicated. Reliable data is needed to determine whether there is a need for alarm and whether any measures should be taken to enhance the digital resilience of small and medium-sized Dutch retail stores (Fafinski et al., 2010, p. 6;

Veenstra et al., 2015, p. 4+15; Van der Kleij et al., 2020, p. 114). If so, it would be helpful to know which considerations prevent small and medium-sized Dutch retail stores from adopting (more) basic cybersecurity measures already at this moment (Centraal Planbureau, 2018, p. 18; Bada & Nurse, 2019, p. 1; Cheng et al., 2020, p. 8; Van der Kleij et al., 2020, p. 114+124). At this point in time, not much appears to be known yet about how to effectively encourage small stores to protect themselves against cybercrime (Centraal Planbureau, 2019a; Van der Kleij et al., 2019).

4.3. Hypotheses

4.3.1. Cybercrime prevalence and cybersecurity behaviour

No formal hypotheses were developed about the prevalence of cybercrime among small and medium-sized Dutch retail stores. Likewise, no formal hypotheses were developed about the extent to which such stores are taking basic cybersecurity measures to protect themselves against cybercrime.

4.3.2. Decision-making about basic cybersecurity measures

Following an extensive literature review, a model was developed that might explain how small and medium-sized retail stores decide (not) to adopt basic cybersecurity measures. Please see figure 3. The model is largely based on the protection motivation theory, which will be described in the remainder of this section. The model was influenced by the rational choice theory (which assumes that people make rational cost-benefit analyses when determining how to behave) as well (Lovett, 2006, p. 240). No formal hypotheses were developed about the relative importance of individual model components in the decision-making processes of small and medium-sized Dutch retail stores.

The protection motivation theory is a brainchild of the American psychologist Ronald Rogers (1975). It was originally developed to explain why people (fail to) adopt behaviours that are known to be good for their health (Rogers, 1975; Maddux & Rogers, 1983; Milne et al., 2000, p. 106-107; Bockarjova & Steg, 2014, p. 277; Hanus & Wu, 2016, p. 3; Warkentin, 2016, p. 26; Anwar et al., 2017, p. 437-438; Jansen & Van Schaik, 2019, p. 41; Van Bavel et al., 2019, p. 30). Since its inception, the protection motivation theory has become “widely adopted as a framework for the

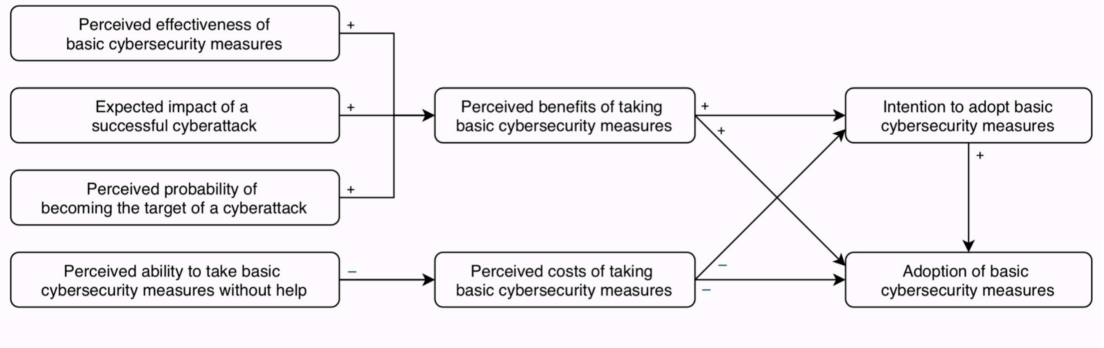
Perceived effectiveness of basic cybersecurity measures
+
Expected impact of a successful cyberattack
+
Perceived probability of becoming the target of a cyberattack
+
Perceived ability to take basic cybersecurity measures without help
–
Perceived benefits of taking basic cybersecurity measures
+
+
Perceived costs of taking basic cybersecurity measures
–
–
Intention to adopt basic cybersecurity measures
+
Adoption of basic cybersecurity measures

Figure 3. The explanatory model that was tested in this study was based on the protection motivation theory.

prediction of and intervention in health-related behavior" (Milne et al., 2000, p. 106). It was heavily influenced by various other theories, such as the health belief model (Edwards, 1954; Bandura, 1977; Milne et al., 2000, p. 108; Anwar et al., 2017, p. 437-438). In the course of time, it was recognised that the protection motivation theory can also be used to explain why people (fail to) adopt self-protective behaviours that are not related to their physical health (Maddux & Rogers, 1983; Bockarjova & Steg, 2014, p. 277). It has been used, for example, to explain why people do or do not decide to prepare for earthquakes and other natural hazards (Milne et al., 2000, p. 110).

The protection motivation theory posits that people decide whether to take certain measures to protect themselves from a specific threat on the basis of four considerations (Bockarjova & Steg, 2014, p. 277; Van Bavel et al., 2019, p. 30). First of all, there are two threat appraisal factors: (A) how probable does one think it is that the threat will materialise, and (B) how severe does one think the consequences of such a turn of events would be? In addition, there are two coping appraisal factors: (C) how confident is one that the recommended measures will protect oneself against the threat, and (D) how confident is one in one's own ability to take those measures? These four factors will be referred to here as 'perceived probability', 'perceived severity', 'perceived effectiveness' and 'perceived ability', respectively. They largely determine whether people will intend to take certain self-protective measures or not, according to the protection motivation theory. People's intention to do something, in turn, is thought to be a key determinant of their actual behaviour (Maddux & Rogers, 1983, p. 470; Anwar et al., 2017, p. 438; Van Bavel et al., 2019, p. 30). Please note that threat and coping appraisal processes can take place both consciously and subconsciously (Bockarjova & Steg, 2014, p. 277).

Can the protection motivation theory be applied in the context of cybercrime and cybersecurity? This is an interesting question. In the literature, it is hotly debated whether traditional criminological theories have any explanatory value in the digital world (Leukfeldt & Yar, 2016, p. 263; Cheng et al., 2020, p. 7). Some scholars believe that they do (Grabosky, 2001, p. 243), whereas others seem to have their doubts (Capeller, 2001; Yar, 2005; Ilievski, 2016, p. 31). Empirical research in this area has mostly focused on strongly established criminological theories like the routine activity theory (Cohen & Felson, 1979; Alshalan, 2006, p. 26; Holt & Bossler, 2008; Ilievski, 2016, p. 34; Leukfeldt & Yar, 2016, p. 263; Junger et al., 2017; Cheng et al., 2020) and the general theory of crime (Bossler & Holt, 2010, p. 234; Ngo & Paternoster, 2011, p. 773). The results have been mixed, and much is still uncertain in this area (Junger et al., 2017, p. 1; Van de Weijer et al., 2019, p. 487). As far as the protection motivation theory is concerned, however, various studies seem to have found (partial) support for the idea that this theory can be applied in the context of cybercrime and cybersecurity (Crossler, 2010, p. 2; Mohamed & Ahmad, 2012, p. 2366; Anwar et al., 2017, p. 438; Jansen & Van Schaik, 2019, p. 41; Martens et al., 2019, p. 139). Almost all of the studies in question focused on only one specific type of cybercrime, however, instead of on cybercrime in general (Martens et al., 2019, p. 139). Besides, it seems that the protection motivation theory has never been examined in the context of cybercrime and cybersecurity at an organisational (rather than an individual) level before. What is true for individuals may not be true for organisations, and vice versa (Li & Siponen, 2011, p. 9; Dang-Pham & Pittayachawan, 2015, p. 282).

5. Methodology

To find answers to the three questions that together formed the foundation of this study, a survey was developed. In line with past recommendations (Moitra, 2004, p. 120), the survey was primarily based on the explanatory model that was introduced in section 4.3.2. The survey also contained items about retail stores' past experience with cybercrime and about their current cybersecurity behaviour. In addition, it included items about various factors that might help us interpret our data. Please see table 1 for an overview of those factors and the sources that inspired us to include them.

As is good practice (Reep-Van den Bergh & Junger, 2018, p. 3-4), it was attempted to formulate all survey items in a clear and unambiguous manner. Before being distributed, the survey was reviewed by two experts in the area of cybercrime and cybersecurity. In addition, the survey was reviewed by five small and medium-sized retail stores in the city of Almelo. Similar procedures were followed by other researchers in the past (Osborn, 2014; Renaud, 2016, p. 13; Bekkers et al., 2020, p. 8).

Please see appendix A for the complete (final version of the) survey. The survey consisted of 46 items that were spread over three easily digestible sections. One of the items, number 6.1, was only presented if the preceding item was responded to in an affirmative manner. Most items were statements that could be responded to on a 6-point Likert scale ranging from 0 ('completely disagree') to 5 ('completely agree'). A scale with an even number of answer options was chosen to force respondents to take a stance. The survey was administered online by means of the Qualtrics software package. Filling out the survey was expected to take approximately 5 to 10 minutes.

The survey was distributed among small and medium-sized retail stores from all over the Netherlands. The term 'retail' was broadly defined here to also include service providers like hairdressers. Five different types of retail stores were invited to take part in this study: clothing stores, eyewear boutiques, florist shops, hair salons, and jewellery stores. With the help of online search engines, their contact details were (manually) collected one by one in the course of various months. Stores were only allowed to participate if it was estimated that they had fewer than 50 employees, that they were not part of a large retail chain, and (to exclude webshops) that they had at least one brick-and-mortar point of sale. In total, 3557 stores (located in 392 different cities and towns) were invited to participate. The first invitations were sent out on 22 April 2021. Around 2 May 2021, reminder messages were sent to all stores that did not seem to have filled out the survey yet and that had not indicated that they were not interested in participation. A second and final set of reminder messages was sent out around 10 May 2021. The survey was closed on 15 May 2021.

Factors that were examined	**Sources of inspiration**
Perceived prioritisation of cybersecurity by other stores	Anwar et al., 2017; Tsai et al., 2016
Perceived prioritisation of cybersecurity by branch organisations	Martens et al., 2019; Tsai et al., 2016
Perceived prioritisation of cybersecurity by the government	Martens et al., 2019; Tsai et al., 2016
In-house knowledge about cybercrime and cybersecurity	Cheng et al., 2020; Hanus & Wu, 2016; Van der Kleij et al., 2019; Yucedal, 2010
Number of employees	Statistics Netherlands, 2019a
Degree of digitalisation	Cheng et al., 2020; Ponsard & Grandclaudon, 2020; Van der Kleij et al., 2019; Verizon, 2020
Online visibility	Alshalan, 2006; Bossler & Holt, 2010; Leukfeldt & Yar, 2016; Marcum et al., 2010
Past experience with cybercrime	Pachur et al., 2012; Riek et al., 2015; Tversky & Kahneman, 1974; Virtanen, 2017
Gender of the person who is in charge	Alshalan, 2006; Anwar et al., 2017; Borghans et al., 2009; Hogarth et al., 2007
Age of the person who is in charge	Van Bavel et al., 2019

Table 1. The survey also included items about ten model-independent factors to help us interpret the data.

As a rule of thumb, large samples tend to be more representative of the population that they are drawn from (and therefore better) than small samples (Fafinski et al., 2010, p. 14; Martínez, 2018, p. 9). It was initially feared that not many retail stores would be willing to participate in this study, however, for various reasons. In general, surveys on cybercrime and cybersecurity – two sensitive topics – often fail to attract many respondents (Osborn, 2014, p. 17; Renaud & Weir, 2016, p. 140; Paoli et al., 2017, p. III; Van der Kleij et al., 2019). In addition, this study's survey was distributed via email, which was expected to cause stores to be hesitant to participate in it. It is widely known that cybercriminals often try to lure people into their traps by sending them seemingly innocuous emails, after all. This study could be mistaken for an attempt by such criminals to identify possible targets. Finally, it should also be noted that this study's survey was distributed in the midst of the COVID-19 pandemic. After a long lockdown period, Dutch retail stores were allowed to reopen their stores on 28 April 2021. It was expected that many of them would be quite busy as a result, and therefore not very motivated to participate in this study. In an attempt to avoid an overly disappointing response rate, six measures were taken: (1) the survey invitations were personalised as much as possible, (2) a €50 gift card of choice was raffled among all participants, (3) potential participants were reminded about the survey up to two times after they had received their initial invitations (as was already mentioned earlier), (4) the survey was designed in such a way that stores could anonymously participate in it, (5) participants were allowed to skip all questions that they deemed too sensitive, and (6) a news item (with a link to the survey) was posted on the official website of the University of Twente and referred to in the invitations.

The survey data was statistically analysed with SPSS Statistics. The ADANCO software package was used to test the explanatory model by means of variance-based structural equation modelling.

6. Results

6.1. Number of responses and respondent demographics

The first set of survey invitations reached only 3449 stores, since 108 of the 3557 collected contact details turned out to be invalid. Some of the collected email addresses did not exist, for example, and some contact forms did not work. In total, 624 retail stores answered at least one question. Roughly half of them, 360 retail stores, fully completed the survey. This implies a response rate of 10.4%. Please see table 2 for an overview. Unfortunately, 9 of the 360 responses had to be discarded: those responses did not seem serious, contained too many missing answers, or were submitted by retail stores that turned out to have more than 50 employees and hence should not have been invited to participate in the first place. The final dataset consisted of 351 valid and useful responses.

- -

Subsector	**Number of invitations**	**Number of responses**	**Response rate**
Clothing stores	689	86	12.5%
Eyewear boutiques	519	65	12.5%
Florist shops	589	45	7.6%
Hair salons	1103	98	8.9%
Jewellery stores	549	65	11.8%
Total	3449	360	10.4%

Table 2. In total, 360 stores fully completed the survey. This boils down to a response rate of roughly 10.4%.

Survey response rates are not reported very often in the literature (Paoli et al., 2017, p. III). This study's response rate of 10.4% appears to be relatively good for research on cybercrime and cybersecurity, however. For comparison, a recent Belgian study in this area (which was conducted before the outbreak of the COVID-19 pandemic) achieved a response rate of only 4.9% (Paoli et al., 2017, p. III). The present study's response rate would have been significantly lower if retail stores would not have received up to two reminder messages about the survey. The initial invitations resulted in merely 85 valid responses. The first set of reminder messages brought this number up to 251 valid responses (+166), and the second set of reminder messages further raised it to 360 valid responses (+109). In total, 59 stores indicated that they were not interested in participating. Roughly half of those stores provided a reason for this. Many of them indicated that they did not have time to participate (34.5%). Others did not feel comfortable filling out a survey about cybercrime and cybersecurity (17.2%) or expected that the questions would be too complicated for them (13.8%).

On average, it took respondents approximately 7 minutes (427 seconds) to fill out the survey. (To calculate this average, 38 outliers were first removed. Those outliers were identified by means of the interquartile range rule with a multiplication factor of 1.5.) The participating stores were spread over 194 different cities and towns all over the Netherlands. On average, they had 5.6 employees (median: 4). Almost all of the participating stores (86.3%) had fewer than 10 employees. The survey was primarily filled out by store owners (92.9%) and store supervisors (4.8%). Of all stores that had a single owner (and chose to disclose information about this in the survey), 54.4% were owned by a male and 45.6% were owned by a female. The ages of those store owners were approximately normally distributed, with most owners (46.2%) being 50 to 59 years old.

6.2. Cybercrime prevalence

In total, 36 stores (10.3%) indicated that they had experienced at least one cybercrime incident in the course of the preceding year. Most of those stores (83.3%, 30 stores in total) indicated that none of those incidents had been successful for the cybercriminals who were involved. The remaining stores (16.7%, 6 stores in total) indicated that at least one of the cybercrime incidents that they had experienced in the course of the preceding year had been successful for the cybercriminals who were involved. This implies an overall victimhood rate of 1.7%. The affected retail stores had mostly fallen victim to hacking (5 cases), malware/viruses (2 cases) and invoice fraud (2 cases). (Please note that each respondent could select multiple types of cybercrime on the survey.) The stores that had only experienced unsuccessful cyberattacks mostly reported incidents that involved phishing (20 cases), malware/viruses (15 cases) and invoice fraud (14 cases).

The participating retail stores had experienced fewer cybercrime incidents than traditional crime incidents (like shoplifting) in the course of the preceding year. Please see figure 4 on the next page. In total, 111 stores (31.6%) had experienced at least one traditional crime incident in the course of the last twelve months. A minority of those stores (27.9%, 31 stores in total) indicated that none of those incidents had been successful for the criminals who were involved. The remaining stores (72.1%, 80 stores in total) indicated that at least one of the traditional crime incidents they had experienced in the course of the preceding year had been successful for the criminals who were involved. This means that the number of traditional crime victims in the sample (80) was more than 13 times as high as the number of cybercrime victims in the sample (6). Not surprisingly, perhaps, most retail stores in the sample (63.5%) indicated that they were more concerned about traditional

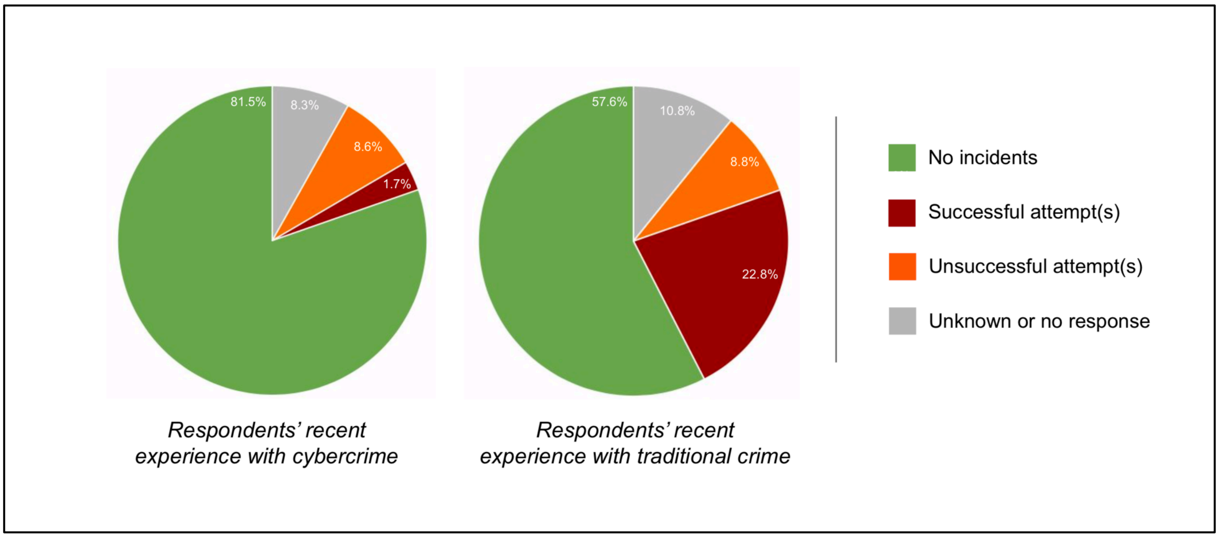

Figure 4. The stores had experienced more traditional crime incidents than cybercrime incidents recently.

crime than about cybercrime. The average agreement score for survey item 8.1 ('We are less worried about cybercrime than about more traditional forms of crime, like shoplifting') was 2.86, which was significantly higher than the middle score of 2.50 (one-sample t-test, p<0.001, 2-tailed).

6.3. Cybersecurity behaviour

The participating stores were asked about seven basic cybersecurity measures. Please see survey items 5.1 to 5.7. The results can be found in figure 5 on the next page. Virtually all respondents indicated that they make use of reliable antivirus software (99.4%) and that they have protected their Wi-Fi networks with a password (98.6%). At the same time, significant proportions of the respondents seem to fail to protect all of their computers with a password (12.1%), install security updates for their software within a week (17.9%), do not grant their customers access to the Wi-Fi networks that they use themselves (20.3%), make back-ups of their most important data at least once a month (26.2%) and replace their passwords at least once a year (57.4%).

A vast majority of all respondents (91.7%) indicated that they are taking at least four of the seven basic cybersecurity measures that they were asked about in the survey. More than a quarter of them (27.1%) even indicated that they are taking all seven of those measures. Please see figure 6 on the next page. At the same time, at least three of the seven basic cybersecurity measures that were asked about in the survey are missing at roughly one fifth of all stores (21.4%). Approximately 44.2% of all respondents indicated that they are missing at least two of those measures, moreover, and a sizeable majority 72.9% indicated that they are missing at least one of them.

In total, 79.9% of all respondents agreed with the statement that small and medium-sized retail stores do not pay a lot of attention to their digital safety (survey item 10.6). Most respondents (52.3%) even agreed with this statement quite vehemently, giving an agreement score of 4 or 5 on a scale from 0 ('completely disagree') to 5 ('completely agree'). The average agreement score was 3.40, which was significantly different from the middle score of 2.50 (one-sample t-test, p<0.001, 2-tailed).

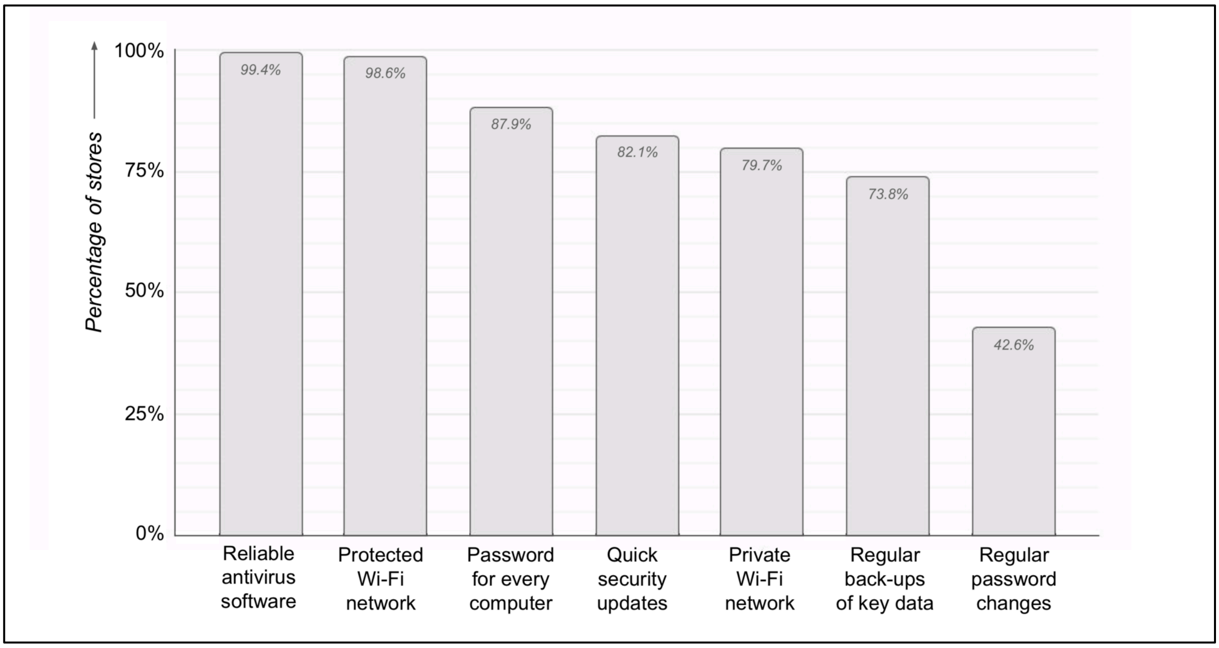

Figure 5. Almost all stores use antivirus software. Fewer than half of them regularly replace their passwords.

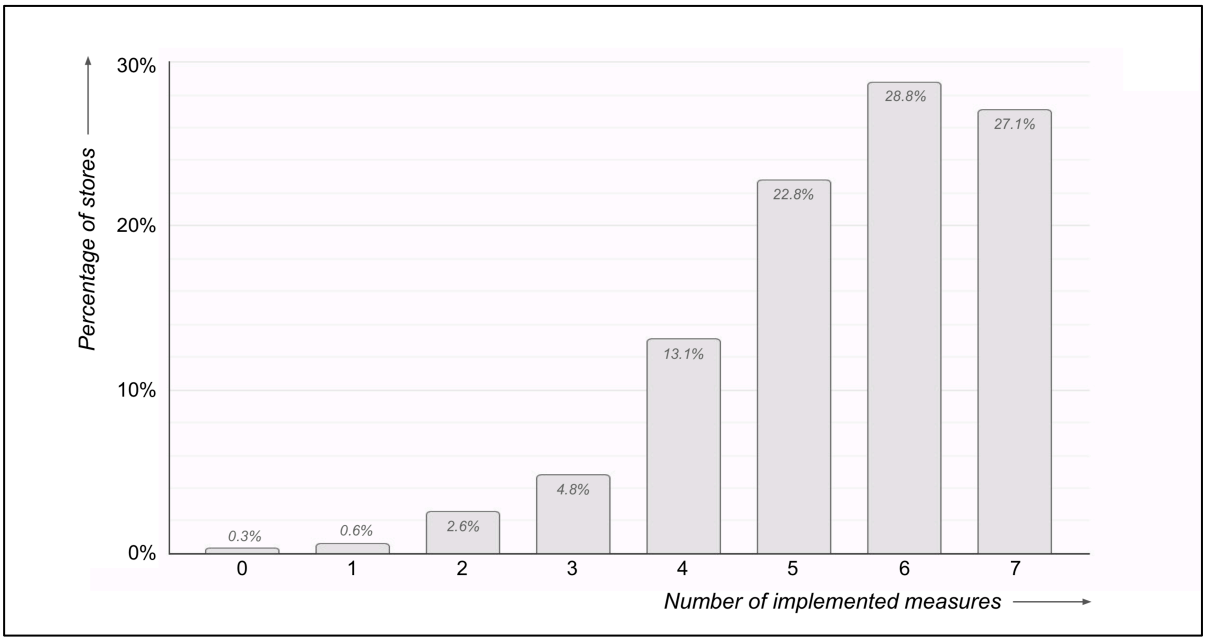

Figure 6. A majority of all stores (72.9%) were found to be missing at least one basic cybersecurity measure.

- -

6.4. Decision-making about basic cybersecurity measures

Please see appendix B for an overview of which survey items served as indicators for which components of the model, and of how those indicators were aggregated into index scores. All components were operationalised as reflective constructs. The dataset was large enough to test the model by means of structural equation modelling: it consisted of 351 unique records, whereas 30 records (10 times the maximum number of arrowheads pointing to a latent variable in the model) would already have been enough to meet the minimum sample size requirement (Hair et al., 2011, p. 144).

6.4.1. Analysis of the outer model

Before the inner model could be tested and interpreted, the outer model's reliability and validity first had to be assessed (Henseler et al., 2009, p. 298; Hanus & Wu, 2016, p. 9). The model's discriminant validity, convergent validity and construct reliability were evaluated one by one.

First of all, the model's discriminant validity was examined. If a set of indicators is used to measure a specific construct in the model, it would be undesirable for that set of indicates to also converge on another construct in the model (Gefen & Straub, 2005, p. 92). To test whether this was the case, heterotrait-monotrait ratio of correlations (HTMT) scores were calculated for each construct pair. They were all (well) below the recommended upper threshold of 0.85 (Henseler et al., 2015, p. 128; Henseler, 2017, p. 26), implying good discriminant validity. A second test looked at the Fornell-Larcker criterion and also found that the discriminant validity was good (Fornell & Larcker, 1981).

Next, the model's convergent validity was examined. Convergent validity is the extent to which an indicator for a certain construct correlates with other indicators for that same construct (Gefen & Straub, 2005, p. 92). To test it, average variance extracted (AVE) scores were calculated for each construct. The AVE scores were greater than 0.50 for most constructs, which is desirable (Henseler, 2017, p. 25). Three constructs had slightly lower AVE scores, however: 'perceived probability' (0.43), 'expected impact' (0.42) and 'adoption' (0.48). Although not ideal, these AVE scores are not extremely low and therefore were not expected to be problematic.

Thirdly and finally, the model's construct reliability was examined. Construct reliability is a measure of the internal consistency of the indicators that are used to measure a construct. Given its superior consistency, Dijkstra-Henseler's ρ was used to evaluate the reliability of each construct in the model (Henseler, 2017, p. 24). The values of ρ were (much) greater than 0.70 for most constructs, which is good. The values of ρ were suboptimal for the constructs 'perceived probability' (0.60) and 'expected impact' (0.60), however. Although again not ideal, these scores were not deemed low enough to be a cause for concern.

6.4.2. Analysis of the inner model

To examine how well the hypothesised explanatory model fitted the collected survey data, a standardised root mean squared residual (SRMR) score was calculated. A value of 0.04 was found, which is well below the recommended upper threshold of 0.08 (Hu & Bentler, 1999; Henseler, 2017, p. 23). An adjusted R^2 value of 0.37 was found for the most important endogenous construct in the model, 'adoption'. This means that roughly 37% of the variance of 'adoption' could be explained by the other constructs in the model (Henseler et al., 2009). This appears to be a decent percentage, given the somewhat exploratory nature of this study and the simplicity of the model (Hanus & Wu, 2016, p. 10). All things considered, the hypothesised model seems to fit the data well.

To learn from the model, its path coefficients were examined. A path coefficient is a standardised regression coefficient that quantifies the direct effect of an independent variable on a dependent variable. Given two such variables, it tells us how the value of the dependent variable would change if the value of the independent variable were to increase by one standard deviation (ceteris paribus) (Henseler, 2017, p. 32). The larger the path coefficient, simply put, the more important the influence of the independent variable on the dependent variable. Please see figure 7 for an overview of all path coefficients that were obtained. Bootstrapping was used to determine whether or not those path coefficients were statistically significant. The outcomes of this process can also be found in figure 7.

The degree to which stores believe that taking basic cybersecurity measures would be beneficial for them appears to be of major influence on the degree to which they (intend to) adopt such basic cybersecurity measures (although it should be noted, of course, that no conclusions about causal effects can be drawn). It seems that stores will be particularly inclined to think that basic cybersecurity measures would be beneficial for them if they believe that a successful cyberattack could have a major impact on them. Stores' perceived effectiveness of basic cybersecurity measures also seems to be of influence here, but (unlike expected) the same does not appear to be true for their views on how likely it is that they will become the target of a cyberattack soon. Stores' views on how costly it would be for them to take basic cybersecurity measures also appear to be of influence on the degree to which they (intend to) adopt such basic cybersecurity measures. They appear to be less influential than stores' views on how beneficial it would be for them to take basic cybersecurity measures, however. The degree to which stores believe that taking basic cybersecurity measures would be costly for them appears to be influenced by their confidence in their own ability to take such measures without any external help.

6.5. Additional findings

6.5.1. Prioritisation of cybersecurity by other parties

The degree to which stores perceive other stores to prioritise cybersecurity (survey item 10.6) was found to be positively correlated with their 'adoption' of basic cybersecurity measures (r=0.180, p=0.001, 2-tailed). It was found to be negatively correlated with their 'perceived effectiveness' (r=-0.131, p=0.017, 2-tailed) and their 'perceived costs' (r=-0.118, p=0.032, 2-tailed).

The average agreement score for survey item 8.3 ('Branch organisations try to encourage small and medium-sized retail companies to enhance their digital resilience') was 2.49, which was not significantly different from the middle score of 2.50. The degree to which stores perceived

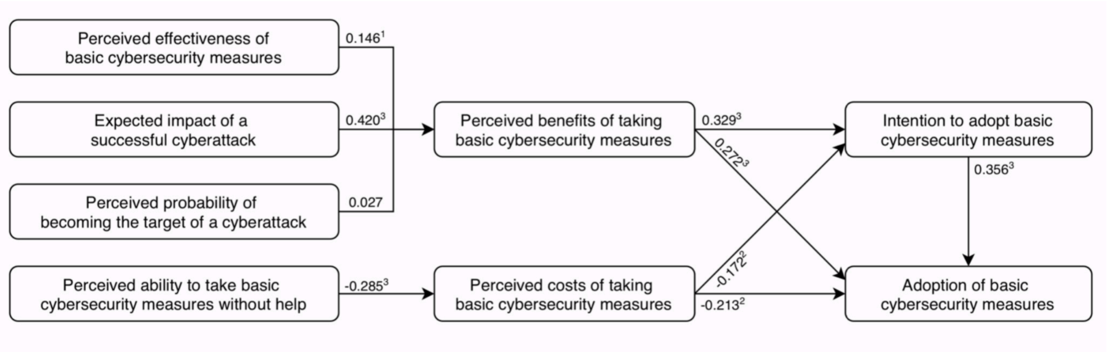
Perceived effectiveness of basic cybersecurity measures
0.146^{1}
Expected impact of a successful cyberattack
0.420^{3}
Perceived probability of becoming the target of a cyberattack
0.027
Perceived ability to take basic cybersecurity measures without help
-0.285^{3}
Perceived benefits of taking basic cybersecurity measures
0.329^{3}
0.272^{3}
Perceived costs of taking basic cybersecurity measures
-0.172^{2}
-0.213^{2}
Intention to adopt basic cybersecurity measures
0.356^{3}
Adoption of basic cybersecurity measures

Figure 7. The outcomes of the ADANCO analyses. Footnotes: (1) p<0.05, (2) p<0.01 and (3) p<0.001.

branch organisations to encourage them to enhance their digital resilience (survey item 8.3) was found to be positively correlated with their 'perceived effectiveness' (r=0.120, p=0.028, 2-tailed), 'perceived ability' (r=0.215, p<0.001, 2-tailed), 'perceived benefits' (r=0.172, p=0.002, 2-tailed), 'intention to adopt' (r=0.127, p=0.021, 2-tailed) and 'adoption' (r=0.318, p<0.001, 2-tailed).

The average agreement score for survey item 8.4 ('The government tries to encourage small and medium-sized retail companies to enhance their digital resilience') was 2.61, which was also not significantly different from the middle score of 2.50. The degree to which stores perceived the government to encourage them to enhance their digital resilience (survey item 8.4) was positively correlated with their 'expected impact' (r=0.163, p=0.002, 2-tailed), 'perceived ability' (r=0.162, p=0.003, 2-tailed), 'perceived benefits' (r=0.179, p=0.001, 2-tailed), 'intention to adopt' (r=0.170, p=0.002, 2-tailed) and (against most prominently) their 'adoption' of measures (r=0.245, p<0.001, 2-tailed). It was negatively correlated with their 'perceived costs' (r=-0.155, p=0.004, 2-tailed).

6.5.2. Knowledge about cybercrime and cybersecurity

The respondents did not seem to be overly confident about their own knowledge about cybercrime and cybersecurity. The average agreement score for survey item 10.5 ('We are well informed when it comes to subjects like cybercrime and cybersafety') was 2.38, which was not significantly different from the middle score of 2.50. The agreement scores were fairly normally distributed.

The degree to which stores were confident about their own knowledge about cybercrime and cybersafety (survey item 10.5) was found to be positively correlated with their 'perceived probability' (r=0.124, p=0.02, 2-tailed), 'perceived effectiveness' (r=0.137, p=0.011, 2=tailed), 'perceived ability' (r=0.321, p<0.001, 2-tailed), 'perceived benefits' (r=0.303, p<0.001, 2-tailed), 'intention to adopt' (r=0.345, p<0.001, 2-tailed) and 'adoption' (r=0.441, p<0.001, 2-tailed). It was found to be negatively correlated with their 'perceived costs' (r=-0.219, p<0.001, 2-tailed).

6.5.3. Degree of digitalisation

Significant positive correlations were observed between stores' degree of digitalisation (survey item 10.1) and their 'expected impact' (r=0.216, p<0.001, 2-tailed), 'perceived benefits' (r=0.206, p<0.001, 2-tailed), 'intention to adopt' (r=0.195, p<0.001, 2-tailed) and 'adoption' (r=0.356, p<0.001, 2-tailed). No significant correlation was found between stores' degree of digitalisation and their 'perceived ability', even though there was a significant negative correlation between stores' degree of digitalisation and their tendency to agree with survey item 3.3 ('Advice about basic cybersecurity measures tends to be too complicated for our company') (r=-0.201, p<0.001, 2-tailed). Survey item 3.3 serves as an indicator for the component 'perceived ability'.

6.5.4. Online visibility

There does not appear to be a significant association between stores' online visibility (survey item 10.4) and how likely they think it is that they will become the target of a cyberattack soon ('perceived probability'). There were significant correlations between stores' online visibility and their 'perceived effectiveness' (r=0.164, p=0.002, 2-tailed), 'perceived benefits' (r=0.179, p=0.001, 2-tailed), 'intention to adopt' (r=0.117, p=0.029, 2-tailed) and 'adoption' (r=0.167, p=0.002, 2-tailed).

6.5.5. Past experience with cybercrime

Stores that had experienced at least one cybercrime incident in the course of the preceding year (survey item 6) scored significantly higher on the model components 'perceived probability' (3.25 vs. 2.39, p<0.001, 2-tailed), 'perceived benefits' (3.36 vs. 2.85, p=0.041, 2-tailed), 'intention to adopt' (3.17 vs. 2.60, p=0.029, 2-tailed) and 'adoption' (3.74 vs. 3.29, p=0.013; 2-tailed) than stores that had not experienced any cybercrime incidents in the course of the preceding year. They also scored significantly lower on the component 'perceived costs' (2.15 vs. 2.67, p=0.011, 2-tailed) than other stores. In addition, stores that had experienced at least one cybercrime incident in the course of the preceding year were significantly less likely to agree with statement 8.1 ('We are less worried about cybercrime than about more traditional forms of crime, like shoplifting') than stores that had not experienced any such incidents during that period (1.92 vs. 3.01, p<0.001, 2-tailed).

On many model components, stores that had fallen victim to a successful cyberattack in the course of the preceding year scored in a manner that is (expected to be) more conducive to cybersecure behaviour than stores that had merely experienced unsuccessful cyberattacks during that period, which in turn scored 'better' than stores that had not experienced any cybercrime incidents at all. Please see table 3. The differences between the average component scores of recent cybercrime victims and the average component scores of stores that had not experienced any cybercrime incidents at all in the course of the past year, were often quite large: roughly one full point on a scale from 0 to 5. Most of the differences between the average component scores of stores that had experienced at least one cybercrime incident in the course of the preceding year and the average component scores of stores that had not experienced any cybercrime incidents during that period, were statistically significant. The only component for which this was not the case, was 'expected impact'.

6.5.6. Store characteristics

Significant positive correlations were found between retail stores' number of employees (survey item 13) and their 'expected impact' (r=0.177, p=0.001, 2-tailed) and 'perceived benefits' (r=0.107, p=0.048, 2-tailed). Perhaps this can be explained by the fact that larger retail stores tend to be more digitalised than smaller ones: a significant correlation was found between retail stores' number of employees and their degree of digitalisation (r=0.169, p=0.001, 2-tailed).

Some notable differences were observed between the five different types of retail stores that took part in the survey. Eyewear boutiques scored higher on 'expected impact', 'perceived benefits' and 'intention to adopt' than all other stores. Florist shops scored higher on 'perceived costs' and lower on 'intention to adopt' than all other stores. These findings can perhaps be explained by looking at the retail stores' degree of digitalisation (survey item 10.1). Eyewear boutiques were more digitalised than all other sores that participated in the survey. Florist shops, on the other hand, were less digitalised than all other stores that participated in the survey.

- -

Recent experience	**'Expected impact'**	**'Perceived probability'**	**'Perceived benefits'**	**'Adoption'**
No cybercrime attempts	2.15	2.39	2.85	3.29
Failed attempts only	2.44	3.21	3.32	3.67
At least one suc. attempt	2.90	3.50	3.60	4.16

Table 3. Stores that had experienced a cybercrime incident recently scored 'better' than stores that had not.

Out of curiosity, it was examined whether there were any correlations between stores' model component scores on the one hand, and the population sizes of the municipalities that those stores were headquartered in on the other. The latter were found to be significantly correlated with stores' 'perceived probability' (r=0.137, p=0.012) and 'adoption' (r=0.121, p=0.026, 2-tailed). Although these correlations are both not very strong, they seem to imply that stores that are headquartered in relatively populated towns and cities think they are more vulnerable to cybercrime and (possibly for that reason) adopt more basic cybersecurity measures than stores that are headquartered in relatively unpopulated towns and cities. These findings could not be explained by looking at stores' degree of digitalisation, online visibility or number of employees. Perhaps small-town stores (subconsciously) believe that cybercrime is a big-city phenomenon. Alternatively, perhaps large-city stores have more connections with other stores than their small-town counterparts, hear more stories about cybercrime incidents through the grapevine as a result, and – potentially as a result of the availability heuristic – consequently become more likely to believe that they could fall victim to a cybercrime incident themselves. Could it also be that cybercrime prevalence is simply higher among stores in relatively populated towns and cities than among stores in relatively unpopulated towns and cities? To test this, the stores were divided into two equally-sized groups: a 'small-town group', and a 'large-city group'. In total, 8.6% of all stores in the 'small-town group' that had provided an answer to survey item 6 had experienced a cybercrime incident in the course of the preceding year. In contrast, 12.7% of all stores in the 'large-city group' that had provided an answer to survey item 6 had experienced a cybercrime incident during the same period. This difference of more than 4 percentage points is remarkable.

6.5.7. Store owner characteristics

Female-led stores (survey item 16) scored significantly higher on 'perceived effectiveness' than male-led stores (4.05 vs. 3.74, p=0.009, 2-tailed). Male-led stores, on the other hand, scored significantly higher on 'intention to adopt' (2.83 vs. 2.49, p=0.038, 2-tailed) and 'adoption' (3.46 vs. 3.24, p=0.048, 2-tailed) than female-led stores. It should be noted that the observed differences were not very large. Perhaps they can be partially explained by the fact that male-led stores were more likely to be (relatively digitalised) eyewear boutiques, whereas female-led stores were more likely to be (relatively undigitalised) hair salons or florist shops.

A significant (albeit weak), positive correlation was found between store owners' age (survey item 17) and their stores' score on the model component 'adoption' (r=0.111, p=0.041, 2-tailed). It should be noted that this correlation was caused entirely by store owners' own perceptions of their stores' digital resilience (survey item 4), which is one of the two indicators for the component 'adoption'. No significant correlation was observed between store owners' age and the number of concrete basic cybersecurity measures that their retail stores are taking (survey items 5.1 to 5.7), which is the other indicator for the model component 'adoption'.

6.5.8. Cybersecurity support

A vast majority of all respondents (80.0%) agreed with the statement that the government, branch organisations and other parties should do more to support retail stores in the area of cybersecurity (survey item 8.5). The average agreement score for this statement was 3.50, which was significantly higher than the middle score of 2.50 (one-sample t-test, p<0.001, 2-tailed). Moreover, more than half of all respondents (55.9%) agreed with this statement quite vehemently, giving an agreement score of 4 or 5 on a scale from 0 ('completely disagree') to 5 ('completely agree').

Interestingly, only 9 respondents (2.6%) were familiar with the Dutch government's Digital Trust Center (survey item 9). Although the Dutch government has launched various other initiatives in recent years as well, the Digital Trust Center is its major vehicle to promote cybersecurity among small and medium-sized enterprises in the Netherlands. In 2017, it was announced that the Dutch government would establish this organisation to provide companies with clear, objective cybersecurity advice (Mallens, 2017). The branch organisation for Dutch SMEs "wholeheartedly applauded" this initiative at the time (Mallens, 2017). The Digital Trust Center became active in 2018 (Mallens, 2017; MKB Nederland, 2018). It aims to provide small and medium-sized Dutch companies with basic cybersecurity advice (Centraal Planbureau, 2019b, p. 34+38).

The average agreement score for survey item 8.2 ('There is so much information about cyber-safety on the Internet that we sometimes cannot see the wood for the trees') was 3.13, which was significantly higher than the middle score of 2.50 (one-sample t-test, p<0.001, 2-tailed). In total, 68.6% of the respondents agreed with this statement. Many of them (43.0% of all respondents) even did so quite vehemently, giving an agreement score of 4 or 5.

6.5.9. Miscellaneous

The average agreement score for survey item 10.3 ('Fear of cybercrime prevents us from further embracing digitalisation') was 1.28, which was significantly lower than the middle score of 2.50 (one-sample t-test, p<0.001, 2-tailed). Only 15.8% of all respondents agreed with the statement. Most of them (8.0% of all respondents) did not do so wholeheartedly, given an agreement score of only 3 on a scale from 0 ('completely disagree') to 5 ('completely agree'). On the other hand, 65.2% of all respondents disagreed with the statement quite vehemently, giving an agreement score of only 0 or 1.

In total, 10.8% of all participating stores indicated that they have cybercrime insurance (survey item 11) – a relatively new phenomenon (Martínez, 2018, p. 9). Insured stores were found to be taking more basic cybersecurity measures than uninsured stores (survey items 5.1 to 5.7; 6.11 vs. 5.22). The observed difference was statistically significant (two-samples t-test, p<0.001, 2-tailed).

7. Discussion

7.1. Main conclusions

7.1.1. Cybercrime prevalence

The results of this study seem to imply that cybercrime is not as prevalent among small and medium-sized retail stores in the Netherlands as some previous research in this area would suggest. In 2019, as was discussed in section 4.2, a study on cybercrime and cybersecurity at small retail stores in The Hague found that almost half of all participating stores had experienced a cybercrime incident in the course of the preceding year (Van der Kleij et al., 2019). In contrast, only 10.3% of all retail stores that took part in the present study had experienced such an incident in the course of the preceding twelve months. A large majority of those incidents, moreover, were unsuccessful for the cybercriminals who were involved in them.

It is not clear why the results of this study paint a less alarming picture about the prevalence of cybercrime among small and medium-sized retail stores in the Netherlands than the results of the above-mentioned 2019 study. Perhaps the discrepancy can be explained by the fact that the 2019 study focused on retail stores in a single city. The Hague is a large city, and the results of the present study suggest that cybercrime prevalence might be slightly higher among stores in relatively populated towns and cities than among stores in relatively unpopulated towns and cities. Alternatively, perhaps the discrepancy can be explained by methodological differences. Although both the present study and the 2019 study made use of surveys, there may have been some important variation in how stores were asked about their recent experience with cybercrime. It is hard to assess this, however, since the 2019 study was never reported on in an academic journal.

It should be noted, of course, that the context in which this study was conducted was very different from the context in which the previous 2019 study was conducted. As was briefly alluded to in section 5 already, the present study's survey was distributed in the midst of the COVID-19 pandemic. The Netherlands had already been under the spell of the coronavirus for more than a year when the first stores were invited to participate in this study on 22 April 2021. It seems highly unlikely, however, that this can explain the observed discrepancy between the results of the present study and the results of the study that was conducted in The Hague in 2019. If anything, in fact, the COVID-19 pandemic appears to have caused Dutch cybercrime rates to dramatically increase (Cybercrime Info, 2020; National Coördinator Terrorismebestrijding en Veiligheid, 2020, p. 18; Van Dijke, 2020; Politie Nederland, 2021).

7.1.2. Cybersecurity behaviour

To what degree are small and medium-sized retail stores in the Netherlands taking basic cybersecurity measures to enhance their digital resilience? Again, the results of this study seem to paint a more reassuring picture than the results of some past research. In 2018, as was also discussed in section 4.2, a nationwide study on cybercrime and cybersecurity at Dutch retail stores of all sizes found that many retail stores were failing to take certain basic cybersecurity measures (Detailhandel Nederland, 2018). Only 43% of all respondents made use of antivirus software, for example, and only 40% of them had protected their Wi-Fi networks with a password. In the present study, in contrast, it was found that 99.4% of all respondents made use of reliable antivirus software and that 98.6% of them have protected their Wi-Fi networks with a password.

Again, it is not entirely clear how these differences can be explained. The above-mentioned 2018 study (which also relied on survey research) did not focus exclusively on small and medium-sized retail stores. Unlike the present study, it looked at retail stores with more than 50 employees as well. It seems unlikely that this can explain why the results of the 2018 study were so much more alarming than the results of the present study, however: in general, as was discussed in section 3.3, large Dutch businesses seem to be taking more (not fewer) cybersecurity measures than their smaller counterparts. Private communication with the deputy director of the (now defunct) branch organisation that commissioned the 2018 study has revealed that only 10% of the data that was collected in that study was provided by retail store owners. In contrast, almost 93% of the data that was collected in the present study was provided by retail store owners. Perhaps this discrepancy could partially explain the observed differences (Grant et al., 2014, p. 99). It is also possible that retail stores have purchased antivirus software and have started to protect their Wi-Fi networks with a password *en masse* in recent years, of course, but this does not seem very plausible.

The present study looked at five other basic cybersecurity measures as well, which were found to be implemented (much) less often by the stores in our sample. More than half of all respondents indicated that they do not replace their passwords at least once a year, for instance. Please see figure

5 again. A sizeable majority (72.9%) of all stores were found to be missing at least one of the seven *basic* cybersecurity measures that were looked at in this study. This is a serious cause for concern: it seems many small and medium-sized Dutch retail stores are unnecessarily vulnerable to cybercrime.

7.1.3. Decision-making about basic cybersecurity measures

The results of this study seem to suggest that explanatory model that was introduced in section 4.3.2 can be used to develop a better understanding of why small and medium-sized retail stores in the Netherlands are (not) taking certain basic measures to protect themselves against cybercrime. The model in question was heavily based on the protection motivation theory which, to the best of our knowledge, had never been examined in the context of cybercrime and cybersecurity at an organisational (rather than an individual) level before.

If one wants to effectively encourage small and medium-sized Dutch retail stores to enhance their digital resilience, it seems important to stress both that basic cybersecurity measures could bring them many benefits and that the costs of such measures are not very high. Please see figure 7 again. The large (potential) benefits seem to deserve more emphasis than the low (certain) costs.

To convince stores that it would be beneficial for them to take basic cybersecurity measures, it seems best to focus their attention on the impact that a successful cyberattack could have on them. It would probably also be useful to inform them about the effectiveness of basic cybersecurity measures. Other research has also hinted in this direction in the past (Hanus & Wu, 2016; Tsai et al., 2016, p. 145; Martens et al., 2019, p. 141). Telling stores that it is likely that they will be targeted by cybercriminals soon, on the other hand, will probably not have much effect. This finding was not in line with our prior expectations, although it should be noted that similar results appear to have been encountered in earlier research among private individuals (Woon et al., 2005, p. 375). In addition, past findings already hinted in the direction that ‘expected impact’ is a more important determinant of self-protective behaviour than ‘perceived probability’ (Tsai et al., 2016, p. 145).

To convince stores that taking basic cybersecurity measures would not be very costly for them, it would probably be good to try to enhance their confidence in their own ability to take such measures without any external help. This finding appears to be in line with the results of past research (Crossler, 2010, p. 4), although the evidence in this area appears to be mixed (Hanus & Wu, 2016, p. 5). The factor ‘perceived costs’ has not been studied much in the past, however, in part because it is difficult to operationalise (Martens et al., 2019, p. 141).

7.2. Implications for practice

In many respects, the results of this study paint a less alarming picture about cybercrime and cybersecurity among small and medium-sized retail stores in the Netherlands than the results of earlier research. There does not appear to be much reason for complacency, however. The results suggest that approximately one in every sixty small and medium-sized retail stores in the Netherlands experiences at least one successful cyberattack each year. Moreover, many small and medium-sized Dutch retail stores appear to be unnecessarily vulnerable to cybercrime because they are failing to take certain basic cybersecurity measures. There is still plenty of space for improvement, in sum.

Small and medium-sized Dutch retail stores would be well-advised to enhance their digital resilience, especially given their increasingly high degree of digitalisation and the widespread expectation that cybercrime will become more prevalent at SMEs in the near future (as was discussed in section 3.2). Arguably, branch organisations and the Dutch government should try to help retail stores achieve this. In total, 80% of all stores that participated in this study indicated that they (strongly) desire more external support in the area of cybersecurity. This was in line with the results of past research on cybercrime and cybersecurity at Dutch SMEs in general (Veenstra et al., 2015, p. 15; Notté & Slot, 2017, p. 2).

It should be noted that the Dutch government already spends millions of euros on various cybercrime prevention initiatives each year (Boes & Leukfeldt, 2017, p. 196-197; MKB Nederland, 2017; Centraal Planbureau, 2018, p. 4; Cyber Weerbaarheidscentrum Brainport, n.d.; Weggelaar, n.d.). Think of the Digital Trust Center, for example, which was briefly described in section 6.5.8. Unfortunately, little is known about the effectiveness of these initiatives (Veenstra et al., 2015, p. 15; Centraal Planbureau, 2019b, p. 36-38). The results of the present study suggest that the Digital Trust Center could benefit from some more publicity: only 2.6% of all respondents were familiar with it. Perhaps it would be good for the Dutch government to reduce the number of initiatives that it is investing in, and to pour more money into the Digital Trust Center instead. According to the Dutch Bureau for Economic Policy Analysis, the current abundance of initiatives can lead to "inefficiency or inconsistencies" (Centraal Planbureau, 2019b, p. 37). Besides, it makes it complex for companies to decide where to go to for help. Almost 70% of all respondents in this study indicated that they sometimes get overwhelmed by the huge amount of cybersecurity advice that can be found online. Similar results have been obtained by other scholars in the past (Osborn, 2014, p. 10; Mijnhardt et al., 2016, p. 106; Renaud, 2016, p. 11+15; Renaud & Weir, 2016, p. 137; Akhgar et al., 2019, p. 196; Bada & Nurse, 2019, p. 5-6; Benz & Chatterjee, 2020, p. 532). It would probably help businesses if there would be a single (public) authority that could provide them with all of the cybersecurity support they need (Armin et al., 2015, p. 14; Renaud, 2016, p. 16; Renaud & Weir, 2016, p. 140; Bada & Nurse, 2019, p. 6-7; Carías et al., 2020, p. 174218). The Digital Trust Center could take on this role in the Netherlands.

Some small and medium-sized Dutch retail stores may need to be convinced that it would be advantageous for them to start taking more basic cybersecurity measures. The results of this study could be used to design effective awareness campaigns. Please see section 7.1.3 again. Awareness campaigns should probably stress that successful cyberattacks can have a large impact on stores. In addition, they should aim to enhance stores' confidence in their own ability to take more basic cybersecurity measures, and they should emphasise that such basic measures – however insubstantial they may seem – can significantly reduce the probability that one will fall victim to cybercrime.

7.3. Strengths and limitations

Arguably, the present study had various strengths. A carefully designed survey was used, for example, which was developed on the basis of an extensive literature review. The survey was distributed among a large, diverse group of small and medium-sized retail stores from all over the Netherlands. As a result, the stores that ended up participating in this study were probably more representative of the population that they were drawn from than would have been the case if a convenience sample had been used (Paoli et al., 2017, p. VII). To reduce self-selection bias as much as possible (Veenstra et al., 2015, p. 6), a gift card was raffled among all participants who shared their email addresses with us (Osborn, 2014, p. 1). Moreover, invitees were reminded about the survey up to two times. Such an "intensive reminding process" is believed to reduce self-selection bias (Reep-Van den Bergh & Junger, 2018, p. 4). Another strength of the present study, is that it attempted to measure both stores' 'intention to adopt' and their actual 'adoption'. This was deemed important since, although the protection motivation theory posits that people's 'intention to adopt' is a key determinant of their actual 'adoption', there is "a known gap" between both constructs (Van Bavel et al., 2019, p. 30; Sheeran & Web, 2016, p. 503). Many past studies that examined the protection motivation theory in the area of cybercrime and cybersecurity failed to measure both of them (Van Bavel et al., 2019, p. 30).

Of course, the present study had various limitations as well. To start, although several efforts were made to reduce self-selection bias as much as possible, it cannot be ruled out that the stores that decided to participate in this study were not entirely representative of all small and medium-sized retail stores in the Netherlands. Perhaps the stores that decided to participate in the study were more interested cybercrime and cybersecurity than the stores that decided not to do so, for example (Veenstra et al., 2015, p. 6). Alternatively, perhaps stores that had recently experienced a cybercrime incident were more suspicious about this study and hence less likely to participate in it than stores that had not experienced any cybercrime incidents recently. Another limitation of this study is the fact that it fully relied on self-reported data (Van Bavel et al., 2019, p. 30). Instead of asking stores to rate their own digital resilience, it would have been better to let experts independently assess their cybersecurity behaviour. Past findings suggests that people tend to act less securely online than they would care to admit to researchers (Van der Kleij et al., 2020, p. 119). To reduce the impact of social desirability effects, the survey was made anonymous. Perhaps this helped: the participating stores do not seem to have answered the survey items in an overly self-flattering manner. Please see section 6.5.2 again, for example. A third limitation of this study is the fact that the cybersecurity measures that were looked at were mostly technical in nature. Soft measures, like teaching employees about cybercrime and setting rules for them on how to behave online, were not examined.

7.4. Suggestions for future research

Three suggestions for future research can be made. Fist of all, future work could investigate cybercrime and cybersecurity in other business sectors that are important to the Dutch economy. It would be interesting to examine whether any cross-sector differences can be observed in this area. If so, perhaps valuable insights could be gained by observing the best-performing sectors. Secondly, future studies could further examine the applicability of the protection motivation theory in the context of cybercrime and cybersecurity at small and medium-sized enterprises. To the best of our knowledge, this was the first study to test that applicability. More research in this area, including in-depth research of a qualitative nature, would be welcome. Thirdly and finally, future work could aim to develop and evaluate an awareness campaign on the basis of the outcomes of this study.

8. Conclusion

The rise of modern technology has brought mankind many benefits, but it has also given rise to new types of threats. Both individuals and organisations can fall victim to cybercrime. They would be well-advised to enhance their digital resilience by taking basic cybersecurity measures, therefore. The present study looked at cybercrime and cybersecurity in the Dutch retail sector. It had three broad aims. First of all, it aimed to establish how prevalent cybercrime is among small and medium-sized retail stores in the Netherlands. Secondly, it aimed to establish to what extent such stores are taking basic cybersecurity measures to protect themselves against cybercrime. Finally, it aimed to explain why some small and medium-sized Dutch retail stores are taking more basic cybersecurity measures than others. A survey was distributed among roughly 3500 stores from all over the Netherlands. In total, 351 useful responses were obtained.

The results of this study suggest that cybercrime is not as prevalent among small and medium-sized Dutch retail stores as previous research would suggest: only 10.3% of all respondents had experienced a cybercrime incident in the course of the past year, and many of those incidents had not been successful for the cybercriminals who were involved in them. Unfortunately, the results also suggest that many Dutch retail stores are unnecessarily vulnerable to cybercrime because they are failing to take some basic cybersecurity measures. Although stores seem to be protecting themselves better than previous research would suggest, there is still plenty of space for improvement: almost three quarters of the stores that participated in this study are failing to take at least one of the seven basic cybersecurity measures that were asked about in the survey. Several factors were identified that may play a role in retail stores' decision-making about basic cybersecurity measures. Simply put, (partial) support was found for the applicability of the protection motivation theory in this area. To the best of our knowledge, the applicability of that theory had never been examined at an organisational level before in the context of cybercrime and cybersecurity.

This was the first large-scale study that specifically focused on cybercrime and cybersecurity at small and medium-sized retail stores in the Netherlands. As such, arguably, it has made a valuable contribution to the literature. In spite of its various limitations, this study will hopefully serve as a solid foundation for further research in this area. Ultimately, such research should aim to enhance the digital resilience of vulnerable businesses so they can stay successful for many more years to come.

9. Appendices

9.1. Appendix A (survey)

This is a translation of the original survey, which was administered in Dutch. The original survey is available upon request. For the sake of conciseness, its introduction and conclusion have been omitted from this translation. Participants were allowed to skip all survey items that they felt uncomfortable with. Items 2, 6, 6.1 and 7 were taken from the 2018 study by Detailhandel Nederland.

Section A – Fear of cybercrime

*First of all, we would like to ask you whether or not you believe
that cybercrime constitutes a serious threat for your company.*

1. Please indicate to what extent you agree with the following statements.

1.1. 'It is likely that our company will fall victim to cybercrime in the upcoming year.'
Likert scale (6 points: 'completely disagree' – 'completely agree').

↓

1.2. ‘Our company is not an interesting target for cybercriminals, so we have little to fear.’ *Likert scale (6 points: ‘completely disagree’ – ‘completely agree’).*

1.3. ‘Cybercriminals rarely target small and medium-sized retail companies.’ *Likert scale (6 points: ‘completely disagree’ – ‘completely agree’).*

1.4. ‘The consequences of a successful cyber attack would probably be quite small for our company.’ *Likert scale (6 points: ‘completely disagree’ – ‘completely agree’).*

1.5. ‘In all likelihood, a successful cyber attack would greatly damage our company.’ *Likert scale (6 points: ‘completely disagree’ – ‘completely agree’).*

2. How much money do you thing an average (successful) cyber attack would cost your company? *Multiple choice (‘at most €20,000’, ‘€20,000 to €40,000’, ‘€40,000 to €60,000’, ‘€60,000 to €80,000’, ‘at least €80,000’, other*

Section B – Basic cybersecurity measures

On the Internet, the government, branch organisations and other parties offer free advice about basic cybersecurity measures that companies could take to enhance their digital resilience. Think of measures like (1) regularly making back-ups of your data and (2) activating two-factor authentication for your online accounts. We would like to ask you for your views on (advice about) such basic cybersecurity measures.

3. Please indicate to what extent you agree with the following statements.

3.1. ‘Free advice on how to enhance your company’s digital resilience tends to be very basic and not very useful.’ *Likert scale (6 points: ‘completely disagree’ – ‘completely agree’).*

3.2. ‘By taking basic cybersecurity measures, you can significantly reduce the likelihood that your company will fall victim to cybercrime in the future (or that such victimhood would have a major impact).’ *Likert scale (6 points: ‘completely disagree’ – ‘completely agree’).*

3.3. ‘Advice about basic cybersecurity measures tends to be too complicated for our company.’ *Likert scale (6 points: ‘completely disagree’ – ‘completely agree’).*

3.4. ‘We are capable of (independently) taking almost all basic cybersecurity measures one could think of.’ *Likert scale (6 points: ‘completely disagree’ – ‘completely agree’).*

3.5. ‘Taking basic cybersecurity measures could greatly benefit our company (or already did so in the past/does so now).’ *Likert scale (6 points: ‘completely disagree’ – ‘completely agree’).*

3.6. ‘Taking basic cybersecurity measures is very expensive.’ *Likert scale (6 points: ‘completely disagree’ – ‘completely agree’).*

3.7. ‘Taking basic cybersecurity measures is very time-consuming.’ *Likert scale (6 points: ‘completely disagree’ – ‘completely agree’).*

3.8. ‘Taking basic cybersecurity measures could be very costly (in a broad sense) for our company (or already was so in the past/is so now).’ *Likert scale (6 points: ‘completely disagree’ – ‘completely agree’).*

↓

3.9. 'We are very motivated to take basic cybersecurity measures.'
Likert scale (6 points: 'completely disagree' – 'completely agree').

3.10. 'For our company, the costs of taking basic cybersecurity measures outweigh the benefits of taking them.' *Likert scale (6 points: 'completely disagree' – 'completely agree').*

Next, we would like to ask you which basic measures you are already taking at this moment to reduce the likelihood that your company will fall victim to cybercrime in the future. Your answers are anonymous and will be treated with care.

4. Please indicate to what extent you agree with the following statement. 'We take many basic measures to enhance the digital resilience of our company.' *Likert scale (6 points: 'completely disagree' – 'completely agree').*

5. Are the following statements accurate for your company? Please indicate so for each statement.

5.1. 'We always try to install security updates for our software as soon as possible (usually within one week).' *Multiple choice ('yes', 'no').*

5.2. 'All of our computer systems are password-protected.' *Multiple choice ('yes', 'no').*

5.3. 'We regularly change our passwords (at least once a year).' *Multiple choice ('yes', 'no').*

5.4. 'We make use of reliable antivirus software.' *Multiple choice ('yes', 'no').*

5.5. 'Our Wi-Fi network is password-protected.' *Multiple choice ('yes', 'no').*

5.6. 'Our customers do not have access to the Wi-Fi network that we use ourselves.' *Multiple choice ('yes', 'no').*

5.7. 'We regularly make back-ups of our most important data, such as our customer database (at least once a month).' *Multiple choice ('yes', 'no').*

Section C – Miscellaneous questions

You have reached the final part of the survey. We still have some miscellaneous questions for you.

6. Did you experience cybercrime in the course of the past year? *Multiple choice ('yes, we fell victim to cybercrime', 'yes, cybercriminals made an attempt, but they were unsuccessful', 'no', 'I do not know').*

6.1. Which forms of cybercrime did you come into contact with in the course of the past year? *Multiple choice ('DDoS attack', 'ransomware', 'hacking', 'identity fraud', 'malware/viruses', 'phishing', 'invoice fraud', 'fraud with gift cards'). Multiple options could be selected. A brief definition was provided for each form of cybercrime. This question was only asked if the answer to question 6 started with 'yes'.*

↓

7. Did you experience traditional store crime, like shoplifting, in the course of the past year? *Multiple choice ('yes, we fell victim to traditional store crime', 'yes, criminals made an attempt, but they were unsuccessful', 'no', 'I do not know').*

8. Please indicate to what extent you agree with the following statements.

8.1. 'We are less worried about cybercrime than about more traditional forms of crime, like shoplifting.' *Likert scale (6 points: 'completely disagree' – 'completely agree').*

8.2. 'There is so much information about cybersafety on the Internet that we sometimes cannot see the wood for the trees.' *Likert scale (6 points: 'completely disagree' – 'completely agree').*

8.3. 'Branch organisations try to encourage small and medium-sized retail companies to enhance their digital resilience.' *Likert scale (6 points: 'completely disagree' – 'completely agree').*

8.4. 'The government tries to encourage small and medium-sized retail companies to enhance their digital resilience.' *Likert scale (6 points: 'completely disagree' – 'completely agree').*

8.5. 'The government, branch organisations and other organisations should do more to support retails stores in the area of cybersecurity.' *Likert scale (6 points: 'completely disagree' – 'completely agree').*

9. Are you familiar with the Digital Trust Center of the Ministry of Economic Affairs and Climate Policy? *Multiple choice ('yes', 'no').*

10. Please indicate to what extent you agree with the following statements.

10.1. 'Our company is strongly digitalised.' *Likert scale (6 points: 'completely disagree' – 'completely agree').*

10.2. 'We plan to further digitalise in the future.' *Likert scale (6 points: 'completely disagree' – 'completely agree').*

10.3. 'Fear of cybercrime prevents us from further embracing digitalisation.' *Likert scale (6 points: 'completely disagree' – 'completely agree').*

10.4. 'Our company is very visible on the Internet. We have our own website, for example, and we are active on social media.' *Likert scale (6 points: 'completely disagree' – 'completely agree').*

10.5. 'We are well-informed when it comes to subjects like cybercrime and cybersafety.' *Likert scale (6 points: 'completely disagree' – 'completely agree').*

10.6. 'Many small and medium-sized retail companies do not pay much attention to their digital safety.' *Likert scale (6 points: 'completely disagree' – 'completely agree').*

11. Is your company insured against cybercrime? *Multiple choice ('yes', 'no', 'I do not know').*

↓

12. What is the best way to describe your company? *Multiple choice ('clothing store', 'eyewear boutique', 'florist shop', 'hair salon', 'jewellery store', other).*

13. Approximately how many people does your company employ? Please include both full-time and part-time employees. *Open answer.*

14. What is your role within the company? *Multiple choice ('owner', 'manager', 'IT employee', other).*

15. In which city is (the largest branch of) your company located? *Open answer.*

16. What is the gender of the person who is in charge at your company? *Multiple choice ('male', 'female', other).*

17. How old is the person who is in charge at your company? *Multiple choice ('20 to 30 years', '30 to 40 years', '40 to 50 years', '50 to 60 years', '60 to 70 years', '70 to 80 years', other).* ■

At the end of the survey, we thanked the respondents for their participation and provided them with our contact details. We also provided them with a link to a separate survey, where they could submit their email address to take part in a €50 gift card raffle and receive a summary of our findings.

9.2. Appendix B (model component formulae)

Model component formulae		
Component 1	Description	Perceived effectiveness of basic measures ('perceived effectiveness')
	Formula	C1 = I3.2*
	Remarks	I3.2 and C1 both run from 0 to 5
Component 2	Description	Expected impact of a successful cyberattack ('expected impact'
	Formula	C2 = [(5-I1.4) + I1.5] / 2
	Remarks	I1.4, I1.5 and C2 all run from 0 to 5
Component 3	Description	Perceived probability of a cyberattack ('perceived probability')
	Formula	C3 = [(5-I1.2) + (5-I1.3)] /2
	Remarks	I1.2, I1.3 and C3 all run from 0 to 5
Component 4	Description	Perceived ability to take basic measures ('perceived ability')
	Formula	C4 = I3.4
	Remarks	I3.4 and C4 both run from 0 to 5
Component 5	Description	Perceived benefits of taking basic measures ('perceived benefits')
	Formula	C5 = I3.5
	Remarks	I3.5 and C5 both run from 0 to 5
Component 6	Description	Perceived costs of taking basic measures ('perceived costs')
	Formula	C6 = (I3.6 + I3.7 + I3.8) / 3
	Remarks	I3.6, I3.7, I3.8 and C6 all run from 0 to 5
Component 7	Description	Intention to adopt basic measures ('intention to adopt')
	Formula	C7 = I3.9
	Remarks	I3.9 and I7 both run from 0 to 5
Component 8	Description	Adoption of basic measures ('adoption')
	Formula	$C8 = [I4 + \frac{5}{7} * \hat{I}5] / 2 \quad \textit{where} \quad \hat{I}5 = \sum_{i=1}^{7} I5.i$
	Remarks	I4 and C8 both run from 0 to 5, I5S runs from 0 to 7
* I3.2 refers to a respondent's score on survey item 3.2. Similar notations are used in the other formulae in this table.		

9.3. Appendix C (model component correlation matrix)

Model component correlation matrix

		C1	C2	C3	C4	C5	C6	C7	C8
C1 Perceived effectiveness	Pearson's r	1	-0.01	-0.024	.114**	.169***	-0.083	.150***	.187***
	P-value*	-	0.852	0.661	0.033	0.002	0.127	0.005	0
	N	350	349	350	347	344	343	347	350
C2 Expected impact	Pearson's r	-0.01	1	.342***	-0.013	.325***	-0.062	.132**	0.098
	P-value*	0.852	-	0	0.812	0	0.25	0.014	0.067
	N	349	350	350	347	344	343	347	350
C3 Perceived probability	Pearson's r	-0.024	.342***	1	-0.006	.211***	-.154***	.253***	.137**
	P-value*	0.661	0	-	0.91	0	0.004	0	0.01
	N	350	350	351	348	345	344	348	351
C4 Perceived ability	Pearson's r	.114**	-0.013	-0.006	1	.213***	-.251***	.194***	.291***
	P-value*	0.033	0.812	0.91	-	0	0	0	0
	N	347	347	348	348	343	342	345	348
C5 Perceived benefits	Pearson's r	.169***	.325***	.211***	.213***	1	-.151***	.372***	.398***
	P-value*	0.002	0	0	0	-	0.006	0	0
	N	344	344	345	343	345	338	344	345
C6 Perceived costs	Pearson's r	-0.083	-0.062	-.154***	-.251***	-.151***	1	-.193***	-.285***
	P-value*	0.127	0.25	0.004	0	0.006	-	0	0
	N	343	343	344	342	338	344	341	344
C7 Intention to adopt	Pearson's r	.150***	.132**	.253***	.194***	.372***	-.193***	1	.397***
	P-value*	0.005	0.014	0	0	0	0	-	0
	N	347	347	348	345	344	341	348	348
C8 Adoption	Pearson's r	.187***	0.098	.137**	.291***	.398***	-.285***	.397***	1
	P-value*	0	0.067	0.01	0	0	0	0	-
	N	350	350	351	348	345	344	348	351

* The significance test was 2-tailed.

** This correlation is significant at α=0.05.

*** This correlation is significant at α=0.01.

10. References

Akhgar, B., Saunders, J., Hancock, P., Lyle, A., & Newsham, D. S. S. (2019). CyberCentric: Increasing SME and citizen resilience against cyberattacks. In B. Akhgar (Ed.), *Serious games for enhancing law enforcement agencies* (pp. 195-208). Cham, Switzerland: Springer. ISBN: 978-3-030-29926-2.

Alshalan, A. (2006). *Cyber-crime fear and victimization: An analysis of a national survey* [Doctoral dissertation]. Mississippi State University. https://hdl.handle.net/11668/16977

Anderson, R., Barton, C., Böhme, R., Clayton, R., Ganan, C., Grasso, T., Levi, M., Moore, T., & Vasek, M. (2019). Measuring the changing cost of cybercrime. *Proceedings of the 18th Annual Workshop on the Economics of Information Security,* 1-32. https://doi.org/10.17863/CAM.41598

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69,* 437-443. doi.org/10.1016/j.chb.2016.12.040

Armin, J., Thompson, B., & Kijewski, P. (2015). Cybercrime economic costs: No measure no solution. *Proceedings of the 10th International Conference on Availability, Reliability and Security,* 701-710. https://doi.org/10.1109/ARES.2015.56

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

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191–215. https://doi.org/10.1037/0033-295X.84.2.191

Bauer, J. M., & Van Eeten, M. J. G. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy, 33*(10-11), 706-719. https://doi.org/10.1016/j.telpol.2009.09.001

Bekkers, L., Van der Kleij, R., Schippers, N., & Leukfeldt, R. (2020). *Cyberweerbaarheidsapp MKB: Ontwikkeling van een webapplicatie om de digitale weerbaarheid van het MKB te vergroten.* Centre of Expertise Cyber Security (De Haagse Hogeschool). https://www.shorturl.at/hxyM9

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

Bockarjova, M., & Steg, L. (2014). Can protection motivation theory predict pro-environmental behavior? Explaining the adoption of electric vehicles in the Netherlands. *Global Environmental Change, 28*, 276-288. https://doi.org/10.1016/j.gloenvcha.2014.06.010

Boes, S., & Leukfeldt, E. R. (2017). Fighting cybercrime: A joint effort. In R. M. Clark & S. Hakim (Eds.), *Cyber-physical security: Protecting critical infrastructure at the state and local level* (pp. 185-203). Cham, Switzerland: Springer. ISBN: 978-3-319-32824-9.

Borghans, L., Golsteyn, B. H. H., Heckman, J. J., & Meijers, H. (2009). Gender differences in risk aversion and ambiguity aversion. *Journal of the European Economic Association, 7(2-3),* 649-658. https://www.jstor.org/stable/40282781

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice, 38*(3)*,* 227-236. https://doi.org/10.1016/j.jcrimjus.2010.03.001

Brustbauer, J. (2016). Enterprise risk management in SMEs: Towards a structural model. *International Small Business Journal, 34*(1), 70-85. https://doi.org/10.1177/0266242614542853

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2020). Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. *European Societies, 23*(S1), 47-59. https://doi.org/10.1080/14616696.2020.1804973

Bureau RMC. (n.d.) *Jaaroverzicht 2018: Pak de consument als je kan!* https://www.rmc.nl/jaaroverzicht-2018-pak-de-consument-als-je-kan/

Capeller, W. (2001). Not such a neat net: Some comments on virtual criminality. *Social & Legal Studies, 10*(2), 229-242. https://doi.org/10.1177/a017404

Carías, J. F., Borges, M. R. S., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). Systematic approach to cyber resilience operationalization in SMEs. *IEEE Access, 8,* 174200-174221. https://doi.org/10.1109/ACCESS.2020.3026063

Centraal Beheer. (2019). *Opvallende uitkomsten cyberonderzoek.* https://nieuws.centraalbeheer.nl/download/637007/centraalbeheer-cybersecurityonderzoekjanuari2019-819448.pdf

Centraal Planbureau. (2018). *Risicorapportage cyberveiligheid economie 2018.* www.cpb.nl/sites/default/files/omnidownload/CPB-Notitie-15okt2018-Risicorapportage-Cyberveiligheid-Economie-2018.pdf

Centraal Planbureau. (2019a). *Betere informatie cruciaal.* https://www.cpb.nl/sites/default/files/omnidownload/def-infographic-CRR2019.pdf

Centraal Planbureau. (2019b). *Risicorapportage cyberveiligheid economie 2019.* https://www.cpb.nl/sites/default/files/omnidownload/cpb-notitie-risicorapportage-cyberveiligheid-2019.pdf

Centrum voor Criminaliteitspreventie en Veiligheid. (2020, September 7). *Ondernemers onderschatten risico's cybercrime.* https://hetccv.nl/nieuws/ondernemers-onderschatten-risicos-cybercrime/

Cheng, C., Chan, L., & Chau, C.-L. (2020). Individual differences in susceptibility to cybercrime victimization and its psychological aftermath. *Computers in Human Behavior, 108,* article 106311. https://doi.org/10.1016/j.chb.2020.106311

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608. https://www.jstor.org/stable/2094589

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

Cyber Weerbaarheidscentrum Brainport. (n.d.) *Over Cyber Weerbaarheidscentrum Brainport.* https://cwbrainport.nl/over-ons/

Cybercrime Info. (2018, October 29). *Cybercrime kan winkelier de kop kosten.* https://www.cybercrimeinfo.nl/cybercrime/281770_cybercrime-kan-winkelier-de-kop-kosten

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

De Groot, N. (2017, September 25). *Jaarlijks 10 miljard schade door cybercrime.* Algemeen Dagblad. https://www.ad.nl/economie/jaarlijks-10-miljard-schade-door-cybercrime~a1e18a70/

Detailhandel Nederland. (2018, October 14). *Internetcriminelen raken winkeliers in het hart.* https://www.detailhandel.nl/nieuws/persbericht-internetcriminelen-raken-winkeliera-in-het-hart

Detailhandel Nederland. (2019). *Jaaroverzicht 2019: Een jaar met verschillende gezichten.* https://www.shorturl.at/yCKR2

Edwards, W. (1954). The theory of decision making. *Psychological Bulletin, 51*(4), 380-417. https://doi.org/10.1037/h0053870

European Commission. (2007). *Towards a general policy on the fight against cyber crime.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52007DC0267

European Commission. (2013). *Cybersecurity strategy of the European Union: An open, safe and secure cyberspace.* https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667

Fafinski, S., Dutton, W. H., & Margetts, H. (2010). Mapping and measuring cybercrime. *Oxford Internet Institute Discussion Papers,* article 18. http://dx.doi.org/10.2139/ssrn.1694107

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50. http://www.jstor.com/stable/3151312

Furnell, S. M. (2001). The problem of categorising cybercrime and cybercriminals. *Proceedings of the 2001 Australian Information Warfare and Security Conference*, 29-36. https://ro.ecu.edu.au/ecuworks/6758

Gañán, C. H., Ciere, M., & Van Eeten, M. (2017). Beyond the pretty penny: The economic impact of cybercrime. *Proceedings of the 2017 New Security Paradigms Workshop,* 35-45. https://doi.org/10.1145/3171533.3171535

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information Systems, 16,* article 5. https://doi.org/10.17705/1CAIS.01605

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies, 10*(2), 243-249. https://doi.org/10.1177/a017405

Grant, K., Edgar, D., Sukumar, A., & Meyer, M. (2014). 'Risky business': Perceptions of e-business risk by UK small and medium sized enterprises (SMEs). *International Journal of Information Management, 34*(2), 99-122. https://doi.org/10.1016/j.ijinfomgt.2013.11.001

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice, 19*(2), 139-151. https://doi.org/10.2753/MTP1069-6679190202

Hanus, B., & Wu, Y. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management, 33*(1), 2-16. https://doi.org/10.1080/10580530.2015.1117842

Hayes, J., & Bodhani, A. (2013). Cyber security: Small firms under fire. *Engineering & Technology, 8*(6), 80-83. https://doi.org/10.1049/et.2013.0614

Hengstz, K., & Van der Grient, R. (2020). *Veilig online 2020: Medewerkers bedrijfsleven (vitaal en niet-vitaal).* Ministerie van Economische Zaken en Klimaat. https://tinyurl.com/mf5nsfhm

Herjavec Group. (2019). *The 2019 official annual cybercrime report.* https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/

Henseler, J. (2017). *ADANCO 2.0.1 user manual.* Composite Modeling. https://www.composite-modeling.com/support/user-manual/

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43,* 115–135. https://doi.org/10.1007/s11747-014-0403-8

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. *Advances in International Marketing, 20,* 277-319. https://doi.org/10.1108/S1474-7979(2009)0000020014

Hogarth, R. M., Portell, M., & Cuxart, A. (2007). What risks do people perceive in everyday life? A perspective gained from the experience sampling method (ESM). *Risk Analysis, 27*(6), 1427-1439. https://doi.org/10.1111/j.1539-6924.2007.00978.x

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1-25. https://doi.org/10.1080/01639620701876577

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20-40. https://doi.org/10.1080/01639625.2013.822209

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling, 6*(1), 1–55. https://doi.org/10.1080/10705519909540118

Ilievski, A. (2016). An explanation of cybercrime victimisation: Self-control and lifestyle/routine activity theory. *Innovative Issues and Approaches in Social Sciences, 9*(1), 30-47. http://dx.doi.org/10.12959/issn.1855-0541.IIASS-2016-no1-art02

Ingraham, D. G. (1980). On charging computer crime. *Computer and Law Journal, 2,* 429-440. https://repository.law.uic.edu/jitpl/vol2/iss1/20/

International Telecommunication Union. (2020). *Measuring digital development: Facts and figures.* https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf

Jaishankar, K. (2018). Cyber criminology as an academic discipline: History, contribution and impact [Editorial]. *International Journal of Cyber Criminology, 12*(1), 1-8. http://dx.doi.org/10.13140/RG.2.2.25117.00488

Jansen, J., & Van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies, 123*, 40-55. https://doi.org/10.1016/j.ijhcs.2018.10.004

Jansen, J., Junger, M., Montoya, L., & Hartel, P. (2013). Offenders in a digitized society. In W. P. Stol & J. Jansen (Eds.), *Cybercrime and the police* (pp. 45-59). The Hague, the Netherlands: Eleven International Publishing. ISBN: 978-94-6236-069-3.

Junger, M., Montoya, L., Hartel, P., & Heydari, M. (2017). Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in Europe. *Presented at the 2017 International Conference on Cyber Situational Awareness, Data Analytics and Assessment.* https://doi.org/10.1109/CyberSA.2017.8073391

Junger, M., Wang, V., & Schlömer, M. (2020). Fraud against businesses both online and offline: Crime scripts, business characteristics, efforts, and benefits. *Crime Science, 9,* article 13. https://doi.org/10.1186/s40163-020-00119-4

KPN. (2020, September 15). *MKB steeds vaker slachtoffer van cybercrime.* https://www.kpn.com/zakelijk/blog/mkb-steeds-vaker-slachtoffer-van-cybercrime.htm

Kuijpers, D., Küpper, J., Tjon Pian Gi, M., & Steins, L. (2016). *Rewriting retail: A sector in acceleration towards 2025.* McKinsey & Company. https://www.vebm.nl/application/files/6515/5299/5334/329885175-Rapport-Retail-Vision-2025.pdf

Kurpjuhn, T. (2015). The SME security challenge. *Computer Fraud & Security, 2015*(3)*,* 5-7. https://doi.org/10.1016/S1361-3723(15)30017-8

Laane, I., Kemps, D., Banning, B., Hofstede, H., Driessen, S., & Van Balen, A. (2021). *Ondernemers onderschatten het risico op cybercriminaliteit.* ABN Amro. https://tinyurl.com/vevdnype

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263-280. https://doi.org/10.1080/01639625.2015.1012409

Li, Y., & Siponen, M. (2011). A call for research on home users' information security behaviour. *Proceedings of the 2011 Pacific Asia Conference on Information Systems,* article 112. http://aisel.aisnet.org/pacis2011/112

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

Lovett, F. (2006). Rational choice theory and explanation. *Rationality and Society, 18*(2), 237-272. https://doi.org/10.1177%2F1043463106060155

Maass, P., & Rajagopalan, M. (2012, August 1). *Does cybercrime really cost $1 trillion?* ProPublica. https://www.propublica.org/article/does-cybercrime-really-cost-1-trillion

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5)*,* 469-479. https://doi.org/10.1016/0022-1031(83)90023-9

Mallens, N. (2017, September 23). *'Opzetten Digital Trust Center helpt bedrijven bij cyberdreiging'.* MKB Nederland. https://www.mkb.nl/nieuws/opzetten-digital-trust-center-helpt-bedrijven-bij-cyberdreiging

Marcum, C. D., Ricketts, M. L., & Higgins, G. E. (2010). Assessing sex experiences of online victimization: An examination of adolescent online behaviors using routine activity theory. *Criminal Justice Review, 35*(4), 412-437. https://doi.org/10.1177%2F0734016809360331

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior, 92,* 139-150. https://doi.org/10.1016/j.chb.2018.11.002

Martínez, I. (2018). *Cyber insurance adoption among Dutch SMEs. An on-field study based on PMT* [Master thesis]. Delft University of Technology. https://www.shorturl.at/rxzBH

Mijnhardt, F., Baars, T., & Spruit, M. (2016). Organizational characteristics influencing SME information security maturity. *Journal of Computer Information Systems, 56*(2), 106-115. https://doi.org/10.1080/08874417.2016.1117369

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology, 30*(1), 106-143. https://doi.org/10.1111/j.1559-1816.2000.tb02308.x

Misra, G., Junger, M., & Montoya, L. (2017). A cross-national study on cybercrime: Incident, suspect and victim characteristics for digital and traditional fraud in the Netherlands and Kolkata, India. *Journal of Forensic Sciences & Criminal Investigation, 4*(2), article 555634. http://dx.doi.org/10.19080/JFSCI.2017.04.555634

MKB Nederland. (2017, November 7). *Mkb-ondernemer vaakst slachtoffer van malware.* https://www.mkb.nl/nieuws/mkb-ondernemer-vaakst-slachtoffer-van-malware

MKB Nederland. (2018, June 8). *Bedrijfsleven steunt website Digital Trust Center (DTC).* https://www.mkb.nl/nieuws/bedrijfsleven-steunt-website-digital-trust-center-dtc

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concern antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior, 28*(6), 2366-2375. https://doi.org/10.1016/j.chb.2012.07.008

Moitra, S. D. (2004). Cybercrime: Towards an assessment of its nature and impact. *International Journal of Comparative and Applied Criminal Justice, 28*(2), 105-123. doi.org/10.1080/01924036.2004.9678719

Morgan, S. (2020, October 26). *Global cybercrime damages predicted to reach $6 trillion annually by 2021.* Cybercrime Magazine. https://cybersecurityventures.com/annual-cybercrime-report-2020/

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2020). Cybersecuritybeeld Nederland 2020. https://www.nctv.nl/binaries/nctv/documenten/publicaties/2020/06/29/cybersecuritybeeld-nederland-2020/Cybersecuritybeeld+Nederland+2020.pdf

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology, 5*(1), 773-793.

Nhan, J., & Bachmann, M. (2010). Developments in cyber criminology. In M. Maguire & D. Okada (Eds.), *Critical issues in crime and justice: Thought, policy, and practice (second edition)* (pp. 164-183). Thousand Oaks (California), United States of America: Sage Publications. ISBN: 978-1-4833-5062-2.

Norris, G., & Brookes, A. (2021). Personality, emotion and individual differences in response to online fraud. *Personality and Individual Differences, 169,* article 109847. https://doi.org/10.1016/j.paid.2020.109847

Notté, R., & Slot, L. (2017). *Hoe cybersecure is het MKB?* Centre of Expertise Cyber Security (De Haagse Hogeschool). https://www.shorturl.at/pqyGI

Odinot, G., Verhoeven, M. A., Pool, R. L. D., & De Poot, C. J. (2017). *Organised cybercrime in the Netherlands: Empirical findings and implications for law enforcement.* Wetenschappelijk Onderzoek- en Documentatiecentrum. http://hdl.handle.net/20.500.12832/179

Osborn, E. (2014). *Business versus technology: Sources of the perceived lack of cyber security in SMEs* [Working paper]. Centre for Doctoral Training in Cyber Security (University of Oxford). https://ora.ox.ac.uk/objects/uuid:4363144b-5667-4fdd-8cd3-b8e35436107e

Pachur, T., Hertwig, R., & Steinmann, F. (2012). How do people judge risks: Availability heuristic, affect heuristic, or both? *Journal of Experimental Psychology: Applied, 18*(3), 314-330. https://doi.org/10.1037/a0028279

Paoli, L., Visschers, J., Verstraete, C., & Van Hellemont, E. (2017). *The impact of cybercrime on Belgian businesses.* Leuven Institute of Criminology (Katholieke Universiteit Leuven). http://dx.doi.org/10.13140/RG.2.2.28940.41602

Politie Nederland. (n.d.) *Slachtoffer van cybercrime? Informatie voor het MKB.* shorturl.at/gnwWZ

Politie Nederland. (2021, May 17). *Geregistreerde misdrijven en aangiften; soort misdrijf, gemeente.* Retrieved June 4, 2021, from data.politie.nl/ - /Politie/nl/dataset/47013NED/table?ts=1611064193622

Ponsard, C., & Grandclaudon, J. (2020). Guidelines and tool support for building a cybersecurity awareness program for SMEs. *Proceedings of the 2019 International Conference on Information Systems Security and Privacy,* 335-357. https://doi.org/10.1007/978-3-030-49443-8_16

Rechtman, Y. (2017, June 24). *Shifting the risk of cybercrime.* CPA Journal. https://www.cpajournal.com/2017/06/19/shifting-risk-cybercrime/

Reep-Van den Bergh, C. M. M., & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science, 7,* article 5. https://doi.org/10.1186/s40163-018-0079-3

Renaud, K. (2016). How smaller businesses struggle with security advice. *Computer Fraud & Security, 2016*(8), 10-18. https://doi.org/10.1016/S1361-3723(16)30062-8

Renaud, K., & Weir, G. R. S. (2016). Cybersecurity and the unbearability of uncertainty. *Proceedings of the 2016 Cybersecurity and Cyberforensics Conference,* 137-143. https://doi.org/10.1109/CCC.2016.29

Riek, M., Böhme, R., & Moore, T. (2015). Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing, 13*(2), 261-273. https://doi.org/10.1109/TDSC.2015.2410795

Reyns, B. W., & Henson, B. (2015). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology*, 1-21. http://dx.doi.org/10.1177/0306624X15572861

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

Saleem, J., Adebisi, B., Ande, R., & Hammoudeh, M. (2017). A state of the art survey: Impact of cyber attacks on SME's [sic]. *Proceedings of the 2017 International Conference on Future Networks and Distributed Systems,* article 52. https://doi.org/10.1145/3102304.3109812

Sheeran, P., & Webb, T. L. (2016). The intention-behavior gap. *Social and Personality Psychology Compass, 10*(9), 503-518. https://doi.org/10.1111/spc3.12265

Smith, Z. M., & Lostri, E. (2020). *The hidden costs of cybercrime.* McAfee. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

Statistics Netherlands. (n.d.) *Cybercrime achterhalen in aangiften.* https://www.cbs.nl/nl-nl/over-ons/innovatie/project/cybercrime-achterhalen-in-aangiften

Statistics Netherlands. (2019a). *Cybersecuritymonitor 2019.* https://www.cbs.nl/-/media/_pdf/2019/37/cybersecuritymonitor-2019.pdf

Statistics Netherlands. (2019b). *The Netherlands on the European Scale 2019: Internet.* https://longreads.cbs.nl/european-scale-2019/internet/

Statistics Netherlands. (2019c). *Veiligheidsmonitor 2019.* https://www.cbs.nl/-/media/_pdf/2020/10/veiligheidsmonitor-2019.pdf

Statistics Netherlands. (2021a). *Cybersecuritymonitor 2020.* https://www.cbs.nl/-/media/_pdf/2021/18/cybersecuritymonitor-2020.pdf

Statistics Netherlands. (2021b, May 31). *Detailhandel, omzetontwikkeling internetverkopen.* Retrieved January 21, 2021, from https://opendata.cbs.nl/#/CBS/nl/dataset/83867NED/table

Stichting Internet Domeinregistratie Nederland. (2020). *Van vertrouwen geven naar eigen verantwoordelijkheid nemen. De 3 belangrijkste cybersecuritytrends voor ondernemers.* https://cutt.ly/imXbA4S

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

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science, 185*(4157), 1124-1131. https://www.jstor.org/stable/1738360

Twisdale, J. A. (2018). *Exploring SME vulnerabilities to cyber-criminal activities through employee behavior and internet access* [Doctoral dissertation]. Walden University. https://scholarworks.waldenu.edu/dissertations/5428/

Valli, C., Martinus, I. C., & Johnstone, M. N. (2013). Small to medium enterprise cyber security awareness: An initial survey of Western Australian businesses. *Proceedings of the 2013 International Conference on Security and Management,* 71-75. https://ro.ecu.edu.au/ecuworkspost2013/858

Van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies, 123,* 29-39. https://doi.org/10.1016/j.ijhcs.2018.11.003

Van de Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking, 20*(7), 407-412. doi.org/10.1089/cyber.2017.0028

Van de Weijer, S. G. A., Leukfeldt, R., & Bernasco, W. (2019). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology, 16*(4), 486-508. https://doi.org/10.1177/1477370818773610

Van der Kleij, R., De Bruin, I., Van 't Hoff-De Goede, S., Ancher, M., & Leukfeldt, R. (2019, March 4). *Cybercriminaliteit leeft niet onder retailers.* Secondant (Centrum voor Criminaliteitspreventie en Veiligheid). https://ccv-secondant.nl/platform/article/cybercriminaliteit-leeft-niet-onder-retailers

Van der Kleij, R., Van 't Hoff-De Goede, S., Van de Weijer, S., & Leukfeldt, R. (2020). Ons cybergedrag is veel onveiliger dan we zelf denken. *Justitiële Verkenningen, 46*(2), 113-128. https://doi.org/10.5553/JV/016758502020046002011.

Veenstra, S., Zuurveen, R., & Stol, W. (2015). *Cybercrime onder bedrijven: Een onderzoek naar slachtofferschap van cybercrime onder het midden- en kleinbedrijf en zelfstandigen zonder personeel in Nederland.* Cyber Science Center. cybersciencecenter.nl/media/1054/2015-05-13-cybercrime-onder-bedrijven-def.pdf

Verbano, C., & Venturini, K. (2013). Managing risks in SMEs: A literature review and research agenda. *Journal of Technology Management & Innovation, 8*(3), 186-197. https://doi.org/10.4067/S0718-27242013000400017

Verizon. (2020). *Data breach investigations report 2020.* https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf

Virtanen, S. M. (2017). Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities. *Psychiatry, Psychology and Law, 24*(3), 323-338. https://doi.org/10.1080/13218719.2017.1315785

Wanamaker, K. A. (2019). *Profile of Canadian businesses who report cybercrime to police.* Public Safety Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2019-r006/2019-r006-en.pdf

Wang, S. S. (2019). Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal, 57,* article 101173. https://doi.org/10.1016/j.pacfin.2019.101173

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems, 92,* 25-35. doi.org/10.1016/j.dss.2016.09.013

Weggelaar, A. (n.d.). *City deal lokale weerbaarheid cybercrime.* Centrum voor Criminaliteitspreventie en Veiligheid. https://hetccv.nl/onderwerpen/cybercrime/city-deal-lokale-weerbaarheid-cybercrime/

West, R. (2008). The psychology of security. *Communications of the Association for Computing Machinery, 51*(4), 34-40. https://doi.org/10.1145/1330311.1330320

Weulen Kranenbarg, M., Holt, T. J., & Van Gelder, J.-L. (2019). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behavior, 40*(1), 40-55. https://doi.org/10.1080/01639625.2017.1411030

Wiederhold, B. K. (2014). The role of psychology in enhancing cybersecurity [Editorial]. *Cyberpsychology, Behavior, and Social Networking, 17*(3), 131-132. https://doi.org/10.1089/cyber.2014.1502

Woon, I. M. Y., Tan, G. W., & Low, R. T. (2005). A protection motivation theory approach to home wireless security. *Proceedings of the 26th International Conference on Information Systems,* article 31. https://aisel.aisnet.org/icis2005/31

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407-427. https://doi.org/10.1177/147737080556056

Yucedal, B. (2010). *Victimization in cyberspace: An application of routine activity and lifestyle exposure theories* [Doctoral dissertation]. Kent State University. rave.ohiolink.edu/etdc/view?acc_num=kent1279290984

Zhang, L., Young, R., & Prybutok, V. (2007). Inhibitors of two illegal behaviors: Hacking and shoplifting. *Journal of Organizational and End User Computing, 19*(3), 24-43. https://doi.org/10.4018/joeuc.2007070102