The awareness and victimization of cybercrime amongst SME's in Twente.

Author: Susan Bezemer
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands

ABSTRACT,
It is impossible to imagine your life without computers or smartphones anymore. Everything today happens digitally, and Web 2.0 is currently taking place. Even though being online all the time has countless advantages, it also opens up a world of online criminality, which can be called cybercrime. This study focuses on the awareness and victimization of cybercrime amongst small to medium sized enterprises (SME's) in Twente. The study was conducted in Enschede and involved 54 SME's, whom filled out an online questionnaire about the awareness of cybercrime within their business and about their experience with cybercrime. It was found that many of the businesses are not aware of the potential risks they could encounter and only a few would take further actions if they were involved in cybercrime. However, businesses are more likely to take action, if financial damage is involved.

Graduation Committee members:
Prof. Dr. Marianne Junger
S. Abhishta

Keywords

Cybercrime; SME; victimization; Routine Activity Theory; awareness.

11th IBA Bachelor Thesis Conference, July 10th, 2018, Enschede, The Netherlands.

1. INTRODUCTION

It is impossible to imagine your life without computers or smartphones anymore. Everything today happens digitally, and Web 2.0 is currently taking place. There are countless advantages which can be linked to this digital world, but there are also downsides to being online all the time. Online criminality, which can be called cybercrime, is increasing (Crowe, 2018). In 2015 in the Netherlands, one in nine people were victims of cybercrime (CBS, 2017). Besides the dangers of cybercrime for society, it is also becoming clearer that businesses should be aware of these dangers too: one in five companies are victims of cybercrime (CBS, 2017). The yearly Economic Crime Survey from PWC writes that cybercrime is one of the fastest growing type of fraud in businesses and some specialists say that cybercrime will become one of the biggest risks for business in the future (Mikkers, Boere, Van Florestein, & Van Zijl, 2017). These numbers illustrate why it is more than ever important to focus on cybercrime as a potential business problem. Even though the importance of cybercrime is not something that has been discovered just yet and it has been around for quite some time, there is still so much to discover in this department. Since it is getting clearer how dangerous cybercrime can be for businesses of all sizes, the need for this type of research is increasing. Gathering more information about the awareness of cybercrime amongst businesses and about the level of victimization that these businesses experience, might help give a better overview of how dangerous cybercrime really is for a business. Therefore, the goal of this research is to focus on small to medium sized businesses and the dangers of cybercrime for them.

The above-mentioned research goal leads to the following research questions: *"To what extent are small and medium-sized enterprises (SME's) in Twente aware of the risks of cybercrime for their business and what are the effects of cybercrime on victimized businesses."*
In order to answer the research question, the following sub questions can be formulated:

1. Cybercrime and SME's
    i. What is cybercrime?
    ii. What are small to medium-sized enterprises?
    iii. What are the known risks of cybercrime for small to medium-sized enterprises?
2. To what extent do small to medium-sized enterprises become victims of cybercrime?
3. What are the damages of small to medium sized enterprises who were victimized by cybercrime?
4. What safety precautions do small to medium sized enterprises take against cybercrime?

2. LITERATURE REVIEW

In order to answer the previously mentioned research question, a literature review will be carried out. By doing a literature review, it will be possible to gather more information about the subject and about previously done studies. This literature will be collected via the University of Twente library, Google Scholar, Scopus and Web of Science. The following keywords will be used: "cybercrime", "business" and "SME".

2.1 Defining cybercrime

According to Merriam Webster (2018), cybercrime can be defined as a crime, such as theft, fraud, intellectual property violations or the distribution of child pornography, committed electronically (Cybercrime, (n.d.)). This is a very compact definition of the word and for this research, a more elaborative definition is needed. Computer-related crime, shortly cybercrime, is a long-established phenomenon. According to Chawki, Darwish, Ayoub Khan and Tyagi, cybercrime is "any criminal activity that involves a computer either as an instrument, target or a means for perpetuating further crimes comes within the ambit of cybercrime." (Chawki, Darwish, Ayoub Khan, & Tyagi, 2015, p. 3)

Cybercrime can be split up into two aspects: computer-assisted crime and computer-focused crime. The first, computer-assisted crime, can be defined as classic crimes, that are now being conducted within the cyberspace. Examples of this are online scamming, online extortion and online identity theft (Veenstra, Zuurveen, Jansen, Kloppenburg, & Stol, 2014). Computer-focused crime can be defined as a crime in which the use of a computer are not only the means to commit the crime, but also the ends. Examples of this are DDoS attacks and hacking (Veenstra, Zuurveen, Jansen, Kloppenburg, & Stol, 2014). In this research, both computer-assisted crime and computer-focused crime will be taken into account. The reasons for this are the limited resources and therefore limited possibilities to distinguish between the different type of crimes.

Organizations more often see cybercrime as a threat for their business (Klahr, et al., 2017). In 2017, three-quarters of the UK businesses say that cyber security is a high priority for their senior management (Klahr, et al., 2017). In the same study, 46% of all UK businesses encountered at least one cybercrime experience in the last 12 months. Among medium sized firms, this was 66% (Klahr, et al., 2017). According to Klahr et al. (2017), those cybercrime experiences happen most at firms who have cyber security as a low priority (Klahr, et al., 2017). The type of crimes that happen most, are fraudulent e-mails (72%), viruses, spyware and malware (33%) and identity theft, where people are impersonating the organization via e-mail or online (27%) (Klahr, et al., 2017).

A different research from the Haagse Hogeschool, conducted their research among 800 MKB's in the Netherlands. This study shows that 51% said that they have never been victims of cybercrime. Moreover, 21% said that there had been a failed attempt of a cybercrime. Twenty percent of the respondents have been a victim of cybercrime and the remaining 8% says they do not know if they have been a victim (Notté & Slot, 2017). The MKB's mostly were victims of malware (30%) or ransomware (17%) (Notté & Slot, 2017).

2.2 Defining SME's

In order to conduct the research within the right sample, it is necessary to first define what is meant with a SME. There are several definitions that try to define this. The European Commission says that a SME can be defined by two factors: 1) staff headcount and 2) turnover or balance sheet total (European Commission, 2018). Because of the limited availability of indicators such as turnover and balance sheet total, it was decided to not use the definition of the European Commission for this research. Instead, this research will focus only on the staff headcount. According to most Dutch definitions, a SME exists out of 1 to 250 employees. Since this study will be conducted within the Netherlands, it was decided to use this as the foundation of the definition of a SME. However, it is assumed that there might be a substantial difference between a one-person business and a business existing out of 250 employees. For the reliability of this research, the definition of a SME is slightly adapted. The

samples within this research will be organizations existing out of 1 to 70 employees.

2.3 Routine Activity Theory

In order to test the awareness of businesses on the risks of cybercrime, the Routine Activity Theory (RAT) will be used. RAT is a theory that is used to explain why crime happens (Cohen & Felson, 1979). According to Cohen & Felson (1979), the RAT exists out of three elements. These elements are 1) a suitable target, 2) a motivated offender and 3) the absence of a capable guardian against a violation (Cohen & Felson, 1979). If there is a lack of any of these three elements, it will be impossible to have a successful completion of the crime (Cohen & Felson, 1979). If there is an intersection of these three elements, the probability of a crime happening, is increasing (Cohen & Felson, 1979).

As mentioned above, the RAT exists out of three elements. The target (of the crime) can be anything, but as for this research, the target will be the business or the owners of the business. A motivated offender can be anyone: it can be an ex-employee who tries to sabotage the owner, it can be a hacker who wants valuable customer information, or it can be someone who fakes an employee's identity**.** As for a capable guardian, it can be a firewall, the owner, the police or any other kind of security protection for the business. If the capable guardian is missing, the target is lacking protection against the motivated offender and is therefore exposed to a crime.

The RAT has been widely used, but as the read literature describes, only in terms of individuals (Holt & Bossler, 2008). In this research, the theory will be used to describe why crime happens for a business, especially a SME, and not an individual. Furthermore, the use of RAT in the previous literature was focused on crime in general. With the growth of the internet and therefore also victims of online criminality, some studies looked into the use of RAT to describe the victimization of cybercrime (Pratt, Holtfreter, & Reisig, 2010). In this study, RAT will be used for cybercrime only.

As described above, RAT has not been used in business context very often. Some studies do mention RAT in terms of businesses and cybercrime and their results are the following. Holt & Bossler (2008), describe RAT in terms of victimization of online harassment. According to their study, being more computer literate and having more computer skills, does not act as a protective factor against experiencing online harassment (Holt & Bossler, 2008). Furthermore, neither owning a computer nor the speed of one's Internet connection increases the odds of being harassed online (Holt & Bossler, 2008). General computer use and activities, do not have a significant impact on being harassed online (Holt & Bossler, 2008). Demographic preferences, which are often being used in targeting regular crime victims, cannot be directly observed online and therefore this is not relevant. According to Pratt, Holtfreter and Reisig (2010), cyber criminals target consumers during the course of their regular Internet routines (Pratt, Holtfreter, & Reisig, 2010).

Furthermore, according to Lin (2006), direct-to-consumer marketing communication channels such as the Internet, might be efficient, it may also create unguarded exposure to online criminality. (Lin, 2006). The creation of online databases, in which businesses (often retailers) store customer information (e.g. names, addresses, passwords, credit/debit cards and/or bank details), have become a lucrative target for fraudsters (Newman & Clarke, 2003).

In the study of Pratt, Holtfreter & Reisig (2010), it is explained how RAT can be integrated when talking about cybercrime:

> Although routine activity theory predicts that more time spent away from home will increase victimization risk in other contexts (e.g., burglary of an unguarded residence), this proposition is less applicable to Internet fraud targeting, given that consumers often engage in routine online activities (e.g., shopping on Web sites) while in the safe confines of their own homes. What this means is that in the fraud victimization context, staying home and spending time (and money) online exposes potential targets for victimization. (Pratt, Holtfreter, & Reisig, 2010, p. 274)

3. METHODOLOGY

This research will be conducted in Twente. However, the study will mostly take place in Enschede, but it could also be necessary to conduct the questionnaire in cities near Enschede to spread the sample.

To collect data, a structured questionnaire will be carried out. The questions that are asked, can be found in appendix I. Here you can find a overview, in which the questions and answer possibilities are stated. Furthermore, a justification of the used methodology is added. It is important that this justification has been made, since by doing this there will be gained more insight in this research.

This survey will be conducted at small to medium sized businesses in Twente and the answers that are given will help giving answer to the research question. In order to get a clear overview of the sample used in this research; it will be conducted in at least 55 businesses.

The questionnaire consists of questions developed by myself and out of questions based on questionnaires from previous research. All questions are based on read literature. The questions are for a large extent based on the study 'MKB en cybercrime', by S. Veenstra, R. Zuurveen, J. Jansen, S. Kloppenburg and W. Stol. This study focuses on the awareness and victimization of Dutch SME's in a digitalized society. This is quite similar to the research question of this study, only the research environment differs. However, the questionnaire seemed suitable to be used as the foundation of the questionnaire used in this research.

In order to get the sample size, a convenience sample will be conducted. There are two methods that have been used during this research, the first being a 'random walk' concept. During the random walk, I will walk into the stores, ask for the manager and explain to the manager what the research is about. In order to give the manager more information about the research, an official letter will be handed out (appendix II). After the introduction, the manager is asked if there is time to fill out the questionnaire. Expecting it will not be possible to conduct these immediately after the walk-in, there will be made an appointment to conduct the questionnaire or the questionnaire will be sent to their e-mail. This way of collecting data is random, but for this research its purpose, there was decided not to include any big organizations that have multiple offices in the Netherlands since they represent much more than just Twente. Therefore, these stores will not be visited.

In order to spread the possibilities of this research, besides the random walk, the survey will also be posted on Facebook, LinkedIn and other online channels trying to reach more

businesses. I have also used my personal network, by asking friends and family if they know any small to medium sized business in Twente. Furthermore, MKB Twente, which is an association that focuses on SME's within Twente, has been contacted. This association was willing to send the questionnaire via their newsletter to their members and posted a link to the survey on their website (Appendix III) and their social media (Appendix IV). The newsletter has been sent on Thursday 17th of May. The post on social media was placed on Tuesday 22th of May.

3.1 Defining risks

In order to decide which type of cybercrimes will be included in this study, the website "Veilig internetten" was consulted. This website is an initiative from the Dutch government and several big organizations (Nationaal Cyber Security Centrum, 2018). To expand the reach of the study, the list has been updated by some of the crimes that has been taken into account during the research 'MKB en Cybercrime' (Veenstra, Zuurveen, Jansen, Kloppenburg, & Stol, 2014). Only the relevant crimes have been taken into account. The list on "Veilig internetten", also includes child pornography and terrorism as a cybercrime, but because of the focus of this research, those crimes do not seem a priority for SME's. The following list will describe the cybercrimes that will be taking into account during this research. (Nationaal Cyber Security Centrum, 2018); (Veenstra, Zuurveen, Jansen, Kloppenburg, & Stol, 2014).

- Virus
- Phishing
- Botnet
- DDoS attacks
- Malware
- Ransomware
- Identity theft
- Hacking
- Blackmail
- Defacing
- Skimming
- Extortion
- Defamation, slander and libel
- Theft of data(carriers)
- Internet fraud
- Unauthorized use of the organizational network

4. RESULTS

In the following section, the results of the questionnaire will be discussed. By reviewing the results, it will be possible to answer the sub-questions that could not be answered during the literature review. The raw data of the results can be found in appendix V, there have also been made additional tables, which can be found in appendix VI.

4.1 Sample size information

The data collection started on Monday 14th of May 2018 and on the day the data collection stopped, the total amount of respondents was 56. In total, 70 people participated in the research, at which 56 completely finished the survey. This gives a response rate of 80%. The reason of why 20% of the respondents did not start the survey, can have several causes. According to Groves, Dillman, Eltinge & Little (2002), the reason of no response can be because the respondent opened the first page, then left the website or because they had problems opening the survey. It is however, very difficult to discover what went wrong during the process. (Groves, Dillman, Eltinge, & Little., 2002)

Furthermore, the answers of two of the respondents could not be taken into account, since their business did not fit into the in subsection 2.2 mentioned definition of a SME. The following results are based on the answers of 54 employees.

From those 54 employees, 7% (n=4) participated in the research via the link posted by MKB Twente. In 28% (n=15) of the cases, the business consists of 1 employee. This was followed by 2-4 employees, which covered 26% (n=14) of the total. In 74% (n=40) of the time, the respondent was the CEO or the owner of the SME. This was followed by 19% (n=10) that was an employee at the SME and 7% (n=4) that had a managing position.

When asked if the respondent is involved in the safety of computers and internet (ICT) within the organization, 69% (n=37) said no. The remaining 32% (n=17) said yes, meaning they are involved in the safety of computers and internet (ICT) within the organization. The respondent's business environment is mostly the retail sector and personal services, both with 26% (n=14). This was followed by business services, 24% (n=13). When asked if the SME operated mostly as a business to business (B2B) or a business to consumer (B2C) organization, the respondents answered with 41% (n=22) that they are working either on the B2C or on both the B2B and B2C market.

All of the respondents (n=54) answered yes when asked if their organization is using the Internet and when asked if the organization has their own website. It was also asked if the respondents use social media, to which 89% (n=48) said yes. The respondents were asked how often they use internet for prementioned purposes. The results of this question can be found in appendix VI, table 1. The respondents were also asked about their activities on social media. The results can be found in appendix VI, table 2.

When asked if the respondents are informed about the online security of the organization, 39% (n=21) answered that they are 'not completely informed, but also not completely not informed'. This is followed by to 'a small extent', answered by 30% (n=16).

When asked to the respondents to what extent they are involved in trying to prevent cybercrime within the organization, the main answer, 44% (n=24), was 'not at all'. This was followed by to 'a small extent' and 'not to a small, neither a large extent' both with 24% (n=13). It was also asked to what extent the organization is dependent on computers and internet (ICT). To this question, 41% (n=22). Answered that they are to 'a large extent' dependent on the internet. This was followed by 'completely dependent' with 32% (n=17).

The respondents were asked about the amount of confidential information on their organizational network and 33% (n=18) of the respondents, said that they have, to 'a very large extent', confidential information saved on their organizational network or computers. When asked if the respondents are aware of the online safety risks their organization could face, 30% (n=16) of the respondents said not to be aware of these risks. The respondents were asked how important the security of digital, business related information is for their organization. This is 'important' for 41% (n=22) of the respondents. Following, 35% (n=19) said this is 'very important' to them.

4.2 Safety measures taken by SME's against cybercrime

The respondents were also asked if they took any physical safety measures to protect their organization against cybercrime. First, 37% (n=20) said their computers and/or laptops have an identification characteristic, such as a personal

username to login to the server or an identification code on the computer and/or laptop. Following, 56% (n=30) said that their computers and/or laptops are not connected to a cable.

When asked if the organization has taken any technical or policy measures against cybercrime, it became clear that most SME's took technical safety measures against cybercrime (appendix VI, table 3). When asked about the policy measures taken, the answers were mostly that they did not take any (appendix VI, table 4). When asked how confident the respondents are by the safety measures the organization took against cybercrime, 46% (n=25) said that they do not have 'little nor much confidence.'
Furthermore, 32% (n=17) of the respondents have confidence in the organizational safety measures. When asked how satisfied the respondents are with the safety measures taken, 48% (n=26) said they are 'not satisfied nor dissatisfied.'
This was followed by 39% (n=21) that said that they are satisfied. When asked if the organization should take more safety measures against cybercrime, 43% (n=23) said they do not know and 30% (n=16) says yes.

4.3 Victimization of cybercrimes and damages

In order to get more information about the level of victimization among SME's, the 54 respondents are asked if they have ever been a victim of cybercrime. The results to this question are that 74% (n=4) said that they have never been a victim of cybercrime, followed by 15% (n=8) saying they do not know. Furthermore, 4% (n=2) said that they have been a victim within the last 12 months. The remaining 7% (n=4) have been a victim more than 12 months ago.

Next, the respondents were showed several different types of cybercrime (mentioned in subsection 3.1) and asked if they have ever experienced one or more of these. Table 5 (appendix VI) shows if and how often a respondent was victim of a certain cybercrime.

If the respondent answered yes to the question if they ever experienced internet fraud, a follow up question about internet fraud was showed. This question has been shown to two respondents and their answers were that they have been a victim of internet fraud since they bought something but never received the product/service and because they have experienced acquisition fraud.

After asking how often and if a respondent has been a victim of cybercrime, the respondents were asked what the latest cybercrime incident was they experienced. This question has been shown to fourteen respondents. The results can be found in table 6 below.

Table 6

The last cybercrime the SME experienced (n=14)

	Latest cybercrime incident experienced by SME
Extortion	1,9%
Theft of data	1,9%
Fraud/scam	3,7%
Hacking	5,6%
Identity theft	3,7%
Malware	5,6%
Unauthorized use of the organizational network	1,9%
Skimming (where debit card or credit card information is being copied)	1,9%
Total percentage of victimized SME's	25,9%
Total percentage of non-victimized SME's	74,1%

When asked to the victimized respondents whether they know who committed this crime, 64% (n=9) said no. Furthermore, 21% (n=3) said yes, where 7% (n=1) said that they might know who did it. The remaining 7% (n=1) said that they do not know who committed the crime.

To the respondents who said that they (might) know (n=4), it has been asked if they know who did it. Their answers were: an employee (25%, n=1), a customer (25%, n=1) and two times the respondent wrote their own answer, these can be found in Appendix VI, question 29. The 14 respondents have also been asked if they experienced any damage from cybercrime within their organization the past year. The answers to this question are that 64% (n=9) said that they had no damage. Following, 14% (n=2) said they had financial damage. The two respondents who had financial damage were asked how much this was. One said they did not know, one said the financial damage was approximately 2500 euros.

The respondents were asked what they did after they found out about the cybercrime (appendix VI, table 7). Most SME's (29%, N=4) did not take any action after discovering the cybercrime. Furthermore, 21% (n=3) said they took extra safety measures trying to prevent future victimization. The respondents that were victimized, have been asked if they contacted an interest group. Many, 86% (n=12), said they contacted someone else then stated in the answer possibilities and those answers were the following:

- Geen(n=4)
- Politie (n=1)
- Niet (n=4)
- Bank (n=1)
- Goede IT-er voor betere beveiliging (n=1)
- De desbetreffende licentieverstrekker (n=1)

The last questions were about whether the respondent would go to the police when cybercrime would happen within their business. This was showed to every respondent (n=54) again, victimized or non-victimized. To this question, 67% (n=36) said yes, whereas 30% (n=16) said maybe. The remaining 4% (n=2) said no.

Next, the question was asked why or why not the respondent would (or would not) go to the police. Most of the respondents. 33% (n=18), said that this depends on the financial damage. Some respondents (2%, n=1) said that this is no case for the police 2% (n=1). Furthermore, 13% (n=7) of the respondents said that the police will not help you with cases like this or, 6% (n=3), said the police will not be able to find the perpetrator. Some said that the organization will be able to solve the problem by itself, 7% (n=4). Others are afraid of reprisals from the perpetrator (2%, n=1) or damage on their image (2%, n=1). Furthermore, the respondents (11%, n=6) think going to the police would cost them too much effort in time and/or money. Also, some respondents (11%, n=6) are not sure if they would go to the police. However, 46% (n=25) said they would go to the police.

At the end of the survey, the respondents were asked if they still had any comments or questions. In appendix V, question 36, the answers to this question are being showed.

5. CONCLUSION

The main goal of this research was to discover what the risks of cybercrime are for an SME in Twente. Furthermore, this research also looked at the level of victimization within the SME's and the prevention against a possible cyberattack, as well as the awareness among SME's about cybercrime. The results lead to the following conclusion.

It can be said that all of the respondents make use of the internet in their business. This is something that is not very surprising. The growing popularity of the internet makes it impossible for a business to ignore, and the businesses were asked at the start if the questionnaire if they used Internet within their organization. However, this growing popularity also shows that the risks of cybercrime are increasing for an organization. Businesses use the internet for all kind of things and many of these actions are being executed daily. Most of the respondents make use of social media. The weekly use of platforms such as Facebook and LinkedIn, are popular amongst SME's. Contradictory, when asked how involved the businesses are in the safety of the computers and internet within the organization, many said not at all. SME's are not informed about the online security of the business and many are not involved in preventing cyber criminality within the organization, even though their businesses are most of the time dependent on the internet. Furthermore, some of the respondents even say that they have confidential information saved on their organizational network of computers. The respondents admit, that they are not aware of the online safety risks they might encounter, but they do think it is important to protect their organization. When looking at the precautions taken against cybercrime, organizations do take physical and technical safety measures. Policy measures, such as written rules about online payments or how to handle unknown files, are not that implemented within the organizations. Furthermore, many of the respondents are confident and satisfied with the measures taken. However, they are not sure if the organization should take more safety measures against cybercrime.

When asked about the level of victimization within the SME's for the first time, many of the respondents claim to have never been a victim of cybercrime. However, when a follow-up question is asked with a more detailed description of different type of cybercrimes, many of the respondents whom said no to the earlier asked question about victimization, did say that they have been a victim of one of more types of cybercrime. The outcome of these two different questions is very interesting. It gives more information about the awareness of (the different types of) cybercrime and about when an SME thinks they might have become a victim of cybercrime. Following, many SME's are not sure if they have taken enough safety measures against cybercrime. Furthermore, some businesses said that they do not know if they have ever been a victim of cybercrime. An interesting point which could be made is that businesses who have never been a victim of cybercrime, might not know if they are protected enough against cybercrime, even though they might think they are.

Most victimized businesses, have been a victim of hacking or malware. Luckily, only very few experienced (financial) damage from the cybercrime. The lack of financial damage within the victimized businesses could maybe be a reason why only a few of the respondents made contact with a professional to prevent a cyberattack from happening in the future, whether this was the police, bank or a computer specialist. This is confirmed in the question followed after this, when most of the people answer that they might go to the police, but that this depends on the amount of financial damage they experienced.

Concluding from this research, businesses are not completely aware of the risks they might encounter. However, they do have confidence in the actions taken by the organization, even though they are not sure if the organization should try to take more preventative safety measures They think their organization is protected enough, but they are not sure if the organization should take more actions against cybercrime. Many of the businesses in this research, have never been a victim of cybercrime, which might let them think they are protected enough. It is hard to understand for a business how and why they should protect themselves more, if they never experienced cybercrime. Another interesting conclusion is that businesses would protect their organization better, if financial damage was involved.

6. LIMITATIONS

It is important to weigh in the limitations when considering the outcomes of this research. Even though I tried to minimize the limitations as much as possible, some limitations could not have been avoided and need to be discussed. First of all, this research has only been conducted in Twente. To gain more knowledge about the research problem, it might be important to focus on other parts of the Netherlands as well. This leads to a next limitation: this research was only conducted by businesses with 1 to 70 employees. In order to gain more information and knowledge, this sample size needs to be bigger. Moreover, the research could even be conducted in businesses bigger than 250 employees, since cybercrime is becoming a problem for these organizations as well. Furthermore, there was a limited time span while conducting research, which led to the fact that not every aspect is discussed in this paper in as much detail as I would have wanted. Also, after conducting the questionnaire I did not ask as many questions about the Routine Activity Theory as I would have liked. This might be an interesting topic for future research.

7. ACKNOWLEDGEMENTS

I want to thank my first supervisor, prof. dr. Marianne Junger and S. Abhishta for their guidance and dedication throughout my bachelor thesis. I also want to thank the fifty-six responding companies for offering their scarce time and effort, by filling out the questionnaire. Furthermore, I want to thank MKB Twente, for helping me gather more respondents and for using

their reach to help me gain more exposure, this resulted in interesting answers I did not expect. At last I want to thank my relatives and acquaintances for their personal support during the process of my bachelor thesis, but also during my whole study.

8. REFERENCES

CBS. (2017). *Cybersecuritymonitor 2017, een eerste verkenning van dreigingen, incidenten en maatregelen.* Den Haag: Centraal Bureau voor de Statistiek.

Chawki, M., Darwish, A., Ayoub Khan, M., & Tyagi, S. (2015). Cybercrime, Digital Forensics and Jurisdiction. Switzerland: Springer International Publishing Switzerland.

Cohen, L. E., & Felson, M. (1979, August). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*(Vol. 44), pp. 588-608.

Cohen, L., & Felson, M. (1979, Augustus). Social Change and Crime Rate Trends: A Routine Activity Approach. pp. 588-608.

Crowe, D. (2018). *Increasing cyber-crime attacks 'costing up to $1b a year'.* Retrieved from The Sydney Morning Herald: https://www.smh.com.au/politics/federal/increasing-cyber-crime-attacks-costing-up-to-1b-a-year-20180410-p4z8ui.html

Cybercrime. ((n.d.)). Retrieved from Merriam-Webster's Law dictionary: https://www.merriam-webster.com/legal/cybercrime

European Commission. (2018, 04 04). *What is an SME?* Retrieved from http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_nl

Groves, R. M., Dillman, D. A., Eltinge, J. L., & Little., R. J. (2002). Survey nonresponse. New York: John Wiley & Sons.

Holt, T. J., & Bossler, A. M. (2008, December 11). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization.

Klahr, R., Shah, J. N., Sheriffs, P., Rossington, T., Pestell, G., Button, M., & Wang, V. (2017). *Cyber security breaches survey 2017.* London: Ipsos MORI Social Research Institute.

Lin, C. A. (2006). Interactive Media Technology and Electronic Shopping. In C. A. Lin, *Communication Technology and Social Change: Theory and Implications.* New York: Routledge.

Mikkers, A., Boere, N., Van Florestein, E., & Van Zijl, S. (2017). *Economic Crime Survey Nederland 2017.* PWC.

Nationaal Cyber Security Centrum. (2018). *Welke soorten cybercrime zijn er?* . Retrieved from Veilig Internetten: https://veiliginternetten.nl/themes/situatie/welke-vormen-van-cybercrime-zijn-er/

Newman, R. G., & Clarke, R. V. (2003). In *Superhighway Robbery: Preventing E-Commerce Crime.* Devon: Willan Publishing.

Notté, R., & Slot, L. (2017). *Hoe cybersecure is het mkb? Nulmeting cybersecurity in het mkb.* Centre of Expertise Cyber Security.

Pratt, T., Holtfreter, K., & Reisig, M. (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory.

Veenstra, S., Zuurveen, R., Jansen, J., Kloppenburg, S., & Stol, W. (2014). *Slachtofferschap onder het Nederlandse Midden- en Kleinbedrijf in een gedigitaliseerde samenleving.* Leeuwarden: Lectoraat Cybersafety, NHL Hogeschool, Politie Academie, Open Universiteit.

9. APPENDICES

Appendix I: Justification of the used methodology.

Question	Answer possibilities	Justification of methodology
1. Hoeveel medewerkers telt uw organisatie, inclusief uzelf?	Single response, semi-closed question. ☐ 1 medewerker. ☐ 2 t/m 4 medewerkers. ☐ 5 t/m 9 medewerkers. ☐ 10 t/m 19 medewerkers. ☐ 20 t/m 29 medewerkers. ☐ 30 t/m 39 medewerkers. ☐ 40 t/m 49 medewerkers. ☐ 50 of meer medewerkers, namelijk… [open text field]	This question makes it possible to distinguish between the different respondents by the size of their organization.
2. Wat is uw functie binnen de organisatie waarvoor u werkt?	Single response, closed question. ☐ Directeur, eigenaar. ☐ Manager. ☐ Medewerker.	This question makes it possible to distinguish between the different respondents by their function within the organization.
3. Houdt u zich bezig met de veiligheid van computers en internet (ICT) binnen de organisatie?	Single response, closed question. ☐ Ja, ik houd mij bezig met de veiligheid van computers en internet (ICT) binnen de organisatie. ☐ Nee, ik houd mij niet bezig met de veiligheid van computers en internet (ICT) binnen de organisatie.	This question makes it possible to distinguish between the different respondents by their use of computers and internet within the organization.
4. Kies de branche die het best past bij (de belangrijkste werkzaamheden van) uw organisatie:	Single response, closed question. ☐ Bouw. ☐ Detailhandel ☐ Financieel. ☐ Groothandel. ☐ Horeca. ☐ Industrie. ☐ Persoonlijke diensten. ☐ Vervoer. ☐ Zakelijke dienstverlening.	This question makes it possible to distinguish between the different respondents by their organization's working sector.
5. Begeeft uw organisatie zich op de consumenten- en/of bedrijvenmarkt?	Single response, closed question. ☐ Consumentenmarkt. ☐ Bedrijvenmarkt (zowel profit- als non-profitorganisaties). ☐ Consumenten- en bedrijvenmarkt.	This question makes it possible to distinguish between the different respondents by their organization's focus on the market, whether this is on consumers and/or businesses (B2B, B2C and/or both).
6. Kunt u in enkele woorden beschrijven wat u bedrijf doet?	Single response, open question.	This question makes it possible to distinguish between the different respondents by their organization's actions.
7. Wordt er binnen uw organisatie gebruik gemaakt van internet?	Single response, closed question. ☐ Nee. ☐ Ja.	This question helps to gain more information about the use of internet within the organization.
8. Beschikt uw organisatie over een eigen website?	Single response, closed question ☐ Nee. ☐ Ja.	This question helps to gain more information about the companies (potential) own website. Having your own website, could lead to a business being a larger target for cybercrime.

9. Voor welke doeleinden wordt internet binnen uw organisatie gebruikt en hoe vaak?	Multiple response via matrix table, closed question. Respondent can choose out of the following answer possibilities: Niet Minder dan maandelijks Maandelijks Wekelijks Dagelijks Continu (24/7) ☐ Het bijhouden van onze website. ☐ Het verwerken van bestellingen. ☐ Het (zelf) plaatsen van bestellingen. ☐ E-mailen. ☐ Gericht informatie zoeken. ☐ Surfen (ongericht) ☐ Internetbankieren. ☐ Online boekhouding. ☐ Downloaden van muziek, films, en/of software. ☐ Beeldbellen: teleconferencing bijvoorbeeld via Skype ☐ Chatten (tekstueel)	This is a follow up question after question 8. It gives more insight at the use of internet within the organization and shows how often an organization uses the internet for certain activities.
10. Maakt uw organisatie gebruik van social media?	Single response, closed question. ☐ Nee. ☐ Ja.	This question helps to gain more information about the use of social media within the organization.
11. Hoe vaak maakt uw organisatie gebruik van de volgende social media?	Multi response via matrix table, closed question. Respondent can choose out of the following answer possibilities: Niet Minder dan maandelijks Maandelijks Wekelijks Dagelijks Continu (24/7) ☐ Twitter. ☐ Facebook. ☐ Instagram. ☐ LinkedIn. ☐ Videosites zoals YouTube. ☐ Een (discussie)forum. ☐ Een blog.	This question helps to gain more information about the use of social media within the organization, with a specific focus on which social media channels an organization uses most.
12. In hoeverre bent u op de hoogte van de online beveiliging van het bedrijf?	Single response, closed question. ☐ Niet. ☐ In kleine mate. ☐ Niet in kleine mate, maar ook niet in grote mate. ☐ In grote mate. ☐ Volledig.	This question helps to gain understanding about the respondent's knowledge about the online security within the organization.
13. In welke mate houdt u zich bezig met het voorkomen van cybercrime binnen uw bedrijf?	Single response, closed question. ☐ Niet. ☐ In kleine mate. ☐ Niet in kleine mate, maar ook niet in grote mate. ☐ In grote mate. ☐ Volledig.	This question answers if the respondent is involved in the prevention of cybercrime within the organization.

14. Hoe afhankelijk is uw organisatie van computers en internet (ICT)?	Single response, closed question. ☐ Niet. ☐ In kleine mate. ☐ Niet afhankelijk, maar ook niet onafhankelijk ☐ In grote mate. ☐ Volledig.	This question explains how dependent businesses are of computers and internet.
15. In welke mate staat op het bedrijfsnetwerk (of op de computers) van uw organisatie vertrouwelijke informatie opgeslagen, zoals klant-, administratiegegevens en/of informatie over productontwikkeling?	Single response, closed question. ☐ Niet. ☐ In kleine mate. ☐ Niet in kleine mate, maar ook niet in grote mate. ☐ In grote mate. ☐ In zeer grote mate.	This question is asked to gain more information about the level of confidential information that might be stored on the organizational computers. As described in Newman & Clarke (2003), the online storage of customer data, such as names, addresses, passwords, credit/debit cards and/or bank details, results in an organization of becoming a more lucrative target for fraudsters (Newman & Clarke, 2003).
16. In welke mate bent u bekend met de online veiligheidsrisico's die uw organisatie loopt?	Single response, closed question. ☐ Niet. ☐ In kleine mate. ☐ Niet in kleine mate, maar ook niet in grote mate. ☐ In grote mate. ☐ In zeer grote mate.	This question is asked to see if the respondent is familiar with the potential security risks they could encounter.
17. Hoe belangrijk is het beveiligen van digitale, bedrijfsgerelateerde informatie van uw organisatie?	Single response, closed question. ☐ Heel onbelangrijk. ☐ Onbelangrijk. ☐ Niet onbelangrijk, maar ook niet belangrijk. ☐ Belangrijk. ☐ Heel belangrijk.	This question helps us understand if the respondent thinks protecting the digital information within the organization is important.
18. Welke <u>fysieke</u> maatregelen heeft uw organisatie genomen om online risico's zo veel mogelijk uit te sluiten?	Multiple response via matrix table, closed question. Respondent can choose out of the following answer possibilities: Ja Nee Weet ik niet ☐ ICT, zoals computers en servers, is voorzien van een <u>identificatiekenmerk</u> waarmee kan worden achterhaald of deze toebehoort aan het bedrijf (bijvoorbeeld d.m.v. een postcode of inloggegevens). ☐ Computers en/of laptops zijn bevestigd aan een <u>kabel.</u>	This question helps us gain more information about the physical measures the organization has taken against cybercrime. The Routine Activity Theory is being used, since this question explains if the organization is experiencing the absence of a capable guardian, which is one of the three elements that need to happen in order for crime to happen (Cohen & Felson, 1979). A capable guardian in this case are the physical safety measures taken against cybercrime, such as an identification characteristic while using the computers.
19. Welke <u>technische</u> maatregelen heeft uw organisatie genomen om online risico's zo veel mogelijk uit te sluiten?	Multiple response via matrix table, closed question. Respondent can choose out of the following answer possibilities: Ja Nee Weet ik niet	This question helps us gain more information about what kind of technical measures the organization has taken against cybercrime. The Routine Activity Theory is being used, since this question explains if the organization is experiencing the absence of a capable guardian, which is one of the three elements that need

	☐ De computers van de organisatie zijn voorzien van een virusscanner. ☐ De computers en/of het netwerk van de organisatie zijn/is voorzien van een firewall. ☐ Het (draadloze) netwerk is beveiligd. ☐ De software op het bedrijfsnetwerk wordt up-to-date gehouden. ☐ (Internet)activiteiten op het bedrijfsnetwerk worden geregistreerd (gelogd*). ☐ *De logs worden (regelmatig) bekeken/geëvalueerd. ☐ Er worden regelmatig back-ups gemaakt van bestanden op computers en/of het bedrijfsnetwerk.	to happen in order for crime to happen (Cohen & Felson, 1979). A capable guardian in this case are the technical safety measures taken against cybercrime, such as a virus scanner, firewall or updating the software of the organizational network.
20. Welke beleidsmaatregelen heeft uw organisatie genomen om online risico's zoveel mogelijk uit te sluiten?	Multiple response via matrix table, closed question. Respondent can choose out of the following answer possibilities: Ja Nee Weet ik niet ☐ Er is een protocol opgesteld waarin is beschreven hoe te handelen bij cybercrime. ☐ Er is een informatiebeveiligingsbeleid aanwezig (bijvoorbeeld, regels m.b.t. melding en registratie, behandeling van media, uitwisseling van informatie, beveiliging van personeel en fysieke bedrijfsbeveiliging). ☐ Werknemers worden bewust gemaakt van online risico's. ☐ Er zijn regels op schrift gesteld over het gebruik van ICT van privédoeleinden. ☐ Er zijn regels op schrift gesteld voor het doen van online betalingen. ☐ Er zijn regels op schrift gesteld over het omgaan met vertrouwelijke informatie, zoals persoonsgegevens van u, uw medewerkers en/of klanten. ☐ Er zijn regels op schrift gesteld over het openen van onbekende bestanden (zoals bijlagen in e-mails). ☐ Er zijn regels op schrift gesteld over het (op verzoek) afgeven van bedrijfsgegevens.	This question helps us gain more information about what kind of policy measures the organization has taken against cybercrime. The Routine Activity Theory is being used, since this question explains if the organization is experiencing the absence of a capable guardian, which is one of the three elements that need to happen in order for crime to happen (Cohen & Felson, 1979). A capable guardian in this case are the policy measures taken against cybercrime, such as written rules about opening unknown files or giving away business data.

	☐ Er worden regelmatig (veiligheid)controles uitgevoerd.	
21. Hoeveel vertrouwen heeft u in het totaal van de door de organisatie genomen maatregelen om cybercrime (online risico's) te voorkomen?	Single response, closed question. ☐ Heel weinig vertrouwen. ☐ Weinig vertrouwen. ☐ Niet weinig en niet veel vertrouwen. ☐ Veel vertrouwen. ☐ Heel veel vertrouwen.	This question helps to gain more knowledge about the level of trust the respondent has in the measures taken by the organization.
22. Hoe tevreden bent u met de in totaal door de organisatie genomen maatregelen om cybercrime te voorkomen?	Single response, closed question. ☐ Heel ontevreden. ☐ Ontevreden. ☐ Niet ontevreden, niet tevreden ☐ Tevreden. ☐ Heel tevreden.	This question helps to gain more knowledge about how satisfied the respondent is with the measures taken by the organization.
23. Zou uw organisatie meer maatregelen moeten nemen om cybercrime te voorkomen?	Single response, closed question. ☐ Nee. ☐ Ja. ☐ Weet ik niet.	This question helps us gain more knowledge about if the respondent thinks the organization should take more measures against cybercrime.
24. Is uw organisatie wel eens slachtoffer geworden van cybercrime?	Single respons, closed question. ☐ Nee, de organisatie is geen slachtoffer van cybercrime geworden. ☐ Ja, in de afgelopen twaalf maanden. ☐ Ja, meer dan een jaar geleden. ☐ Weet ik niet.	This question helps to gain knowledge about the victimization of the organization.
25. In hoeverre heeft uw organisatie in <u>de afgelopen twaalf maanden</u> te maken gehad met de volgende criminaliteitsvormen	Multiple response via matrix table, closed question. Respondent can choose out of the following answer possibilities: Weet niet Niet mee te maken gehad Eén of meer mislukte pogingen Eén keer slachtoffer Meerdere keren slachtoffer ☐ **Afpersing** via internet (het moeten betalen van geld of goederen door bedreiging en/of geweld. ☐ **Chantage** via internet (het moeten afgeven van geld of goederen door te dreigen met het openbaar maken van een geheim of smaadschrift) ☐ **Denial of Service (DoS-) aanval** (digitale aanvallen op het systeem waardoor deze wordt overbelast en niet meer beschikbaar is, bijvoorbeeld het platleggen van een website). ☐ **Defacing** (het zonder toestemmen veranderen/bekladden, vervangen of vernielen van de website van uw organisatie). ☐ **Diefstal van datadragers** (zoals pc, laptop, usb-sticks).	In order to get more information about this victimization, the respondent is asked what kind of cyber criminality it has encountered in the last 12 months.

	☐ **Diefstal van gegevens** (die niet voor de dader bestemd zijn). ☐ **Hacking** (inbraak op de computersystemen van uw organisatie). ☐ **Identiteitsmisbruik** (het misbruik maken van de identiteitsgegevens van uw organisatie). ☐ **Malware** (infectie van computersystemen middels virussen, trojan horses en/of spyware). ☐ **Ongeautoriseerd gebruik van het bedrijfsnetwerk** (bijvoorbeeld door middel van het downloaden/verspreiden van illegale software, kinderpornografie, spam of het plaatsen van berichten van racistische of discriminerende aard). ☐ **Phishing** (het via digitale middelen – email of social media – met een verzinsel informatie over uw bedrijf ontfutselen via mensen binnen uw organisatie. ☐ **Skimming** (waarbij op onrechtmatige wijze zijn pinpas- of creditcardgegevens van uw organisatie bemachtigd en gekopieerd). ☐ **Skimming** (waarbij daders het pinapparaat van uw organisatie hebben aangepast). ☐ **Smaad/laster via internet** (het via ICT opzettelijk aantasten van de goede naam van uw organisatie). ☐ **Fraude/oplichting** (via internet (financiële) schade opgelopen middels bedrog).	
26. Van welke vorm van oplichting/fraude via internet en/of de mobiele telefoon is uw organisatie slachtoffer geworden? (meerdere antwoorden mogelijk)	Multiple response, semi-closed question. ☐ De organisatie heeft iets verkocht/geleverd, maar nooit het geld ontvangen. ☐ De organisatie heeft iets gekocht, maar het product/de dienst niet ontvangen. ☐ De geleverde dienst en/of het geleverde product is niet van de beloofde kwaliteit, bijvoorbeeld nep, kapot. ☐ Acquisitiefraude en/of spookfacturen: een vorm van oplichting waarbij producten worden aangeboden die geen waarde hebben, of kosten in	This question is only showed if the respondent choose that they have been a victim of "oplichting of fraude" in question 25. By asking this question, we gain more knowledge about what kind of scam or fraud the organization encountered.

	rekening worden gebracht voor diensten die niet zijn geleverd of waarvoor geen opdracht is gegeven. ☐ Voorschotfraude: (hierbij bieden de oplichters het slachtoffer iets waardevols aan. Het slachtoffer moet echter eerst (relatief) kleine onkosten voorschieten voordat hij het aangeboden bedrag of product krijgt. Daarna vragen de fraudeurs steeds grotere bedragen, totdat het slachtoffer al zijn geld kwijt is of afhaakt. Vervolgens is er geen spoor meer te bekennen van de oplichters). ☐ De organisatie heeft ongewenst vastgezeten aan een contract en/of abonnement. ☐ Anders, namelijk… [open tekst field]	
27. Wat is het laatste cybercrime incident dat uw organisatie heeft meegemaakt?	Single response, closed question. ☐ Afpersing. ☐ Chantage. ☐ Denial of Service (DDoS) aanval. ☐ Defacing. ☐ Diefstal van datadragers. ☐ Diefstal van gegevens. ☐ Fraude/oplichting. ☐ Hacking. ☐ Identiteitsmisbruik. ☐ Malware. ☐ Ongeautoriseerd gebruik van het bedrijfsnetwerk. ☐ Phishing. ☐ Skimming (waarbij op onrechtmatige wijze de pinpas- of creditcardgegevens van uw organisatie zijn bemachtigd of gekopieerd). ☐ Skimming (waarbij daders het pinautomaat van uw organisatie hebben aangepast). ☐ Smaad/laster via internet (het via ICT opzettelijk aantasten van de goede naam van de organisatie).	This question helps us gain more information about the last cybercrime incident the organization encountered.
28. Weet uw organisatie wie deze cybercrime heeft gepleegd?	Single response, closed question. ☐ Ja. ☐ Er is een vermoeden. ☐ Nee. ☐ Weet niet.	This question is asked to find out if the respondent knows who was involved in the incident. The Routine Activity Theory is being used, since this question explains if the organization knows if there has been a motivated offender, which is one of the three elements that need to happen in order for crime to happen (Cohen & Felson, 1979).

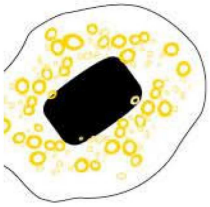
29. Wie heeft (vermoedelijk) de cybercrime gepleegd?	Single response, semi-closed question. ☐ Een medewerker. ☐ Een ex-medewerker. ☐ Een zakenpartner. ☐ Een ex-zakenpartner. ☐ Een klant. ☐ Iemand die ik ken uit mijn zakelijke netwerk. ☐ Iemand die werkt voor een concurrerend bedrijf. ☐ Mijn partner. ☐ Mijn ex-partner. ☐ Een familielid, vriend of andere bekende. ☐ Iemand die ik niet persoonlijk ken. ☐ Anders, namelijk… [open text field]	A follow up question: here the respondent can answer who they think was involved in the cybercrime incident. The Routine Activity Theory is being used, since this question explains if the organization knows who the motivated offender has been (Cohen & Felson, 1979).
30. Welke schade heeft uw organisatie in het afgelopen jaar (2017) ondervonden aan cybercrime?	Single response, semi-closed question. ☐ Geen schade. ☐ Financiële schade. ☐ Verlies en/of beschadiging van gegevens. ☐ Schade in de vorm van tijdverlies. ☐ Imago en/of reputatieschade. ☐ Vertrek van klanten. ☐ Anders, namelijk… [open text field].	In this question it is asked if the respondent experienced any damage from the cybercrime incident and if so, what kind of damage.
31. Hoe groot was de financiële schade (ongeveer)? Afronden op hele bedragen.	Single response, semi-closed question. ☐ [Open text field] euro. ☐ [Open text field] bitcoins. ☐ Weet ik niet. ☐ Zeg ik liever niet.	If financial damage has been selected in the previous question, here we ask how much the damage was.
32. Welke actie(s) heeft uw organisatie ondernomen na het constateren van de betreffende cybercrime? (meerdere antwoorden mogelijk)	Multiple response, semi-closed question. ☐ Mijn organisatie heeft zichzelf geprobeerd schadeloos te stellen/is schadeloos gesteld: de schade is bijvoorbeeld vergoed door een verzekeraar/bank, de handelsite/webwinkel of de dader heeft de ontvreemde goederen teruggegeven. ☐ Mijn organisatie heeft het probleem zelf opgelost, bijvoorbeeld door de eigen IT-afdeling onderzoek uit te laten voeren (de virusinfectie ongedaan maken/het lek dichten). ☐ Mijn organisatie heeft een onafhankelijk onderzoeksbureau (privé; detective/recherche bureau) ingeschakeld om het probleem op te lossen. ☐ Mijn organisatie heeft maatregelen genomen (ervan geleerd) om toekomstig slachtofferschap te voorkomen. ☐ Er is contact gezocht met de politie (bijvoorbeeld om	The following questions are about the actions taken after the cybercrime incident. This helps us gain more information about how the respondents handled the incident and if they took any measures after it.

	melding of aangifte te doen). ☐ Er is contact gezocht met een belangenorganisatie (zoals branchevereniging, Kamer van Koophandel, fraudehelpdesk, etc.). ☐ Er is een juridische dienstverlener ingeschakeld. ☐ Weet niet. ☐ Anders, namelijk… [open tekst field]	
33. Met welke belangenorganisatie is contact gezocht nadat uw organisatie slachtoffer is geworden van cybercrime? (Meerdere antwoorden mogelijk)	Multiple response, semi-closed question. ☐ MKB Nederland. ☐ Kamer van koophandel. ☐ VNO-NCW. ☐ Regionale ondernemersorganisaties en/of brancheorganisaties. ☐ Fraudehelpdesk. ☐ Steunpunt acquisitiefraude. ☐ Anders, namelijk [open text field].	Follow up question. If answered "Er is contact gezocht met een belangenorganisatie (zoals branchevereniging, Kamer van Koophandel, fraudehelpdesk, etc.) ", this question helped specify which organization was contacted.
34. Indien uw organisatie in de toekomst slachtoffer wordt van cybercrime, zou uw organisatie hiervan dan aangifte doen bij de politie?	Single response, closed question. ☐ Nee. ☐ Ja. ☐ Misschien.	This question is asked to find out if the SME's who are victims of cybercrime would contact the police.
35. Waarom zou uw organisatie hiervan (misschien) geen aangifte doen? (Meerdere antwoorden mogelijk)	Multiple response, semi-closed question. ☐ Het hangt af van de hoogte van de (financiële) schade. ☐ Het is vast niet zo belangrijk. ☐ Dit is geen zaak voor de politie. ☐ De politie doet er niets mee. ☐ De politie is niet in staat de dader te vinden. ☐ Het wordt door de organisatie zelf opgelost. ☐ Dan volgen er misschien represailles (=handelingen uit wraak) van de dader. ☐ Dit zorgt mogelijk voor imagoschade. ☐ Dit kost te veel moeite tijd (tijd/geld). ☐ Een andere organisatie dan de politie is hier meer geschikt voor, namelijk… [open text field] ☐ Andere reden, namelijk… [open text field] ☐ Weet ik niet. ☐ Zeg ik liever niet. ☐ Ik zou wel aangifte doen.	Follow up question: when answered no or maybe on the previous question, this question helps to gain more understanding about why an organization would or would not go to the police after a cybercrime incident.
Heeft u zelf nog vragen en/of opmerkingen die u wilt benoemen?	Open question.	Here we give the respondent the possibility to share their thoughts, if they have any.
Bent u hier gekomen via MKB Twente?	Single response, closed question. ☐ Ja. ☐ Nee.	This question is asked to gain knowledge about how many of the respondents found out about the survey via MKB Twente.

Appendix II: Letter with information about the research for the SME's.

UNIVERSITY OF TWENTE.

TO WHOM IT MAY CONCERN



FACULTY OF BEHAVIOURAL, MANAGEMENT AND SOCIAL SCIENCES

VAN
Prof.Dr. M. Junger
T +31 (0)534893207
m.junger@utwente.nl

DATUM
9 mei 2018
ONZE REFERENTIE
IEBIS2018.023

PAGINA
17 of 1

ONDERWERP
Onderzoek

Geachte heer/mevrouw,

De Universiteit Twente doet onderzoek naar cybercrime en cybersecurity en geeft onderwijs op dat gebied.

In dat kader doen wij onderzoek naar slachtofferschap van cybercrime en de online bedreigingen onder winkeliers en MKB-bedrijven en de eventuele voorzorgsmaatregelen hiertegen.

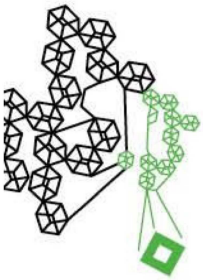
In dit kader zouden wij graag een interview met u willen plannen. Dit interview duurt ongeveer 20-30 minuten en is volledig anoniem.

Na afloop van het interview is er ruimte om verdere vragen te stellen. Het is mogelijk om na afloop van de studie de algemene resultaten te ontvangen.

Mocht u meer informatie willen over ons onderzoek kunt u contact met ons opnemen.

Wij danken u hartelijk voor uw medewerking.

Met vriendelijke groet,



Prof. Marianne Junger
Susan Bezemer

University of Twente
P.O.Box 217, 7500 AE
Enschede The Netherlands www.utwente.nl

Appendix III: Newsletter sent by MKB Twente to their subscribers.

Cybercrime en cybersecurity

De Universiteit Twente doet onderzoek naar cybercrime en cybersecurity en geeft ook onderwijs op dit gebied. In dit kader doen prof. dr. Marianne Junger en Susan Bezemer onderzoek naar slachtofferschap van cybercrime, de online bedreigingen onder winkeliers en MKB-bedrijven en de eventuele voorzorgsmaatregelen hiertegen.

Zij zouden graag een enquête bij u afnemen. Het invullen van deze vragenlijst zal positief bijdragen aan hun onderzoek omtrent cybercrime binnen bedrijven in en om Enschede. Zij waarderen uw hulp enorm!

De enquête is geheel anoniem. Het is mogelijk om, na afronding van het onderzoek, de algemene resultaten te ontvangen. U kunt dan contact opnemen met Susan Bezemer via s.bezemer@student.utwente.nl.

Alvast hartelijk dank voor uw medewerking!

Ik help mee!

Appendix IV: Facebook post by MKB Twente.

Appendix V: Results of the questionnaire via SPSS (Raw data).

Question 1

Hoeveel medewerkers telt uw organisatie, inclusief uzelf? - Selected Choice

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 medewerker.	15	27,8	27,8	27,8
	2 t/m 4 medewerkers.	14	25,9	25,9	53,7
	5 t/m 9 medewerkers.	12	22,2	22,2	75,9
	10 t/m 19 medewerkers.	5	9,3	9,3	85,2
	20 t/m 29 medewerkers.	1	1,9	1,9	87,0
	30 t/m 39 medewerkers.	2	3,7	3,7	90,7
	50 of meer medewerkers, namelijk...	5	9,3	9,3	100,0
	Total	54	100,0	100,0	

When answered '50 of meer medewerkers, namelijk..', the answers were 53, 65, 55, 65 employees.

Question 2

Wat is uw functie binnen de organisatie waarvoor u werkt?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Directeur, eigenaar.	40	74,1	74,1	74,1
	Manager.	4	7,4	7,4	81,5
	Medewerker.	10	18,5	18,5	100,0
	Total	54	100,0	100,0	

Question 3

Houdt u zich bezig met de veiligheid van computers en internet (ICT) binnen de organisatie?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ja, ik houd mij bezig met de veiligheid van computers en internet (ICT) binnen de organisatie.	17	31,5	31,5	31,5
	Nee, ik houd mij niet bezig met de veiligheid van computers en internet (ICT) binnen de organisatie.	37	68,5	68,5	100,0
	Total	54	100,0	100,0	

Question 4

Kies de branche die het best past bij (de belangrijkste werkzaamheden van) uw organisatie:

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Detailhandel.	14	25,9	25,9	25,9
	Financieel.	4	7,4	7,4	33,3
	Groothandel.	5	9,3	9,3	42,6
	Horeca.	2	3,7	3,7	46,3
	Industrie.	2	3,7	3,7	50,0
	Persoonlijke diensten.	14	25,9	25,9	75,9
	Zakelijke dienstverlening.	13	24,1	24,1	100,0
	Total	54	100,0	100,0	

Question 5

Begeeft uw organisatie zich op de consumenten- en/of bedrijvenmarkt?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Consumentenmarkt.	22	40,7	40,7	40,7
	Bedrijvenmarkt (zowel profit- als non-profitorganisaties).	10	18,5	18,5	59,3
	Consumenten- en bedrijvenmarkt.	22	40,7	40,7	100,0
	Total	54	100,0	100,0	

Question 6[1]

"Kunt u in enkele woorden beschrijven wat uw bedrijf doet?"

Het verkopen van schoenen en tassen. Een exclusieve schoenenzaak.	Het verkopen van drogisterijartikelen en parfum.	Lunchroom	Een hip koffietentje, waar je kunt ontbijten, lunchen en een middaghapperijtje kunt doen. Eventueel een wijntje of een biertje doen is ook mogelijk. Uitsluitend Twentse producten met een Molukse twist.	Medische apparatuur en disposables	Creatieve cursussen/workshops in schilderen mozaïek en glas in lood
Schoonheidsbehandelingen	Verkoop kinderkleding	Ontwikkelingen van onlineproducten en diensten.	Coaching op het gebied van beweging, voeding en een gezonde levensstijl.	Financiën beheren van natuurlijke personen die hiertoe zelf niet in staat zijn.	Beschermingsbewind, mentorschap en curatele
Hulpverlening. Dienstverlening.	Juridische zaken	LEAN-trajecten, training en coaching	Begeleiding bij borstvoeding	Totale inrichting van ruimtes	Import en export

[1] For better readability, stylistics and linguistic errors, in the answers given at question 6, have been corrected.

Non-profit: recyclen van producten voor een beter milieu en bewuste samenleving. Verkoop van goede producten voor een super lage prijs. Het bieden van een werkplek aan (vrijwillige) medewerkers om aan de toekomst te werken. Ruimte bieden om zich te ontwikkelen. We helpen dierenwelzijnsorganisaties met de opbrengst.	Accountancy en Belastingadvies	Vertegenwoordigen van diverse mode labels binnen Nederland. Het in de markt zetten van merken, naamsbekendheid creëren bij de retailers in de fashionbranche.	Leveren van kantoorartikelen	Beauty salon	Detacheren van engineers
Voeding- en leefstijlcoaching. Mensen begeleiden naar een gezondere leefstijl.	Marketing, Creatie, Media	Verhuur van stellingen aan particulieren en bedrijven om spullen op te verkopen zonder er zelf bij te staan.	Allround beauty salon, schoonheidssalon, kapsalon, huidtherapie	Autobedrijf	Revisie van verbrandingsmotoren en productie en levering van onderdelen
Ik grossiert in vlees. Ik lever zowel aan slagerijen, horeca als aan de particuliere sector	Preventieve vaccinaties en voorlichting public health	Ik verleen diensten in de verzorging van mensen	Gezondheidscentrum	Werving en selectie en overige personeelsdiensten	Aankoop en ontwikkeling en verhuur van vastgoed
Psychologische en neurofeedback	Verandertrajecten, new business development	Wij zijn een winkel met lingerie en nachtkleding. In de zomer verkopen wij ook badkleding	Juridisch advies Voeren van juridische procedures	Arbodienstverlening Advisering sociale zekerheid vraagstukken	Import en doorlevering van geëxpandeerde klei- en glaskorrels voor bouw, industrie en de groenmarkt
Huid therapeutische behandelingen	Advocatenkantoor	Wij maken kleding op maat en lingerie op maat en wij geven les.	Verkoop van vis	Recruitment	Productiebedrijf in badgoed en bedrijfskleding, 80 % klant specifiek
Optiekbedrijf; verkoop van brillen en zonnebrillen. Aanmeten en leveren van contactlenzen. Tevens verlenen wij oog zorg, bieden optometrische onderzoeken aan.	Kapsalon	Fotografie & grafisch ontwerp	Financiële dienstverlening. Hypotheken, verzekeringen, pensioenen	Verkoop van kaas noten en delicatessen	Nagelproducten verkopen en acrylnagels zetten.

Question 7

Wordt er binnen uw organisatie gebruik gemaakt van internet?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ja.	54	100,0	100,0	100,0

Question 8

Beschikt uw organisatie over een eigen website?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ja.	54	100,0	100,0	100,0

Question 9

Voor welke doeleinden wordt internet binnen uw organisatie gebruikt en hoe vaak? - Het bijhouden van onze website.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet	4	7,4	7,4	7,4
	Minder dan maandelijks	11	20,4	20,4	27,8
	Maandelijks	10	18,5	18,5	46,3
	Wekelijks	11	20,4	20,4	66,7
	Dagelijks	10	18,5	18,5	85,2
	Continu (24/7)	8	14,8	14,8	100,0
	Total	54	100,0	100,0	

Voor welke doeleinden wordt internet binnen uw organisatie gebruikt en hoe vaak? - Het verwerken van bestellingen.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet	18	33,3	33,3	33,3
	Maandelijks	6	11,1	11,1	44,4
	Wekelijks	10	18,5	18,5	63,0
	Dagelijks	15	27,8	27,8	90,7
	Continu (24/7)	5	9,3	9,3	100,0
	Total	54	100,0	100,0	

Voor welke doeleinden wordt internet binnen uw organisatie gebruikt en hoe vaak? - Het (zelf) plaatsen van bestellingen.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet	15	27,8	27,8	27,8
	Minder dan maandelijks	5	9,3	9,3	37,0
	Maandelijks	9	16,7	16,7	53,7
	Wekelijks	11	20,4	20,4	74,1
	Dagelijks	11	20,4	20,4	94,4
	Continu (24/7)	3	5,6	5,6	100,0
	Total	54	100,0	100,0	

Voor welke doeleinden wordt internet binnen uw organisatie gebruikt en hoe vaak? - E-mailen.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet	2	3,7	3,7	3,7
	Wekelijks	4	7,4	7,4	11,1
	Dagelijks	34	63,0	63,0	74,1
	Continu (24/7)	14	25,9	25,9	100,0
	Total	54	100,0	100,0	

Voor welke doeleinden wordt internet binnen uw organisatie gebruikt en hoe vaak? - Gericht informatie zoeken.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet	1	1,9	1,9	1,9
	Maandelijks	3	5,6	5,6	7,4
	Wekelijks	9	16,7	16,7	24,1
	Dagelijks	35	64,8	64,8	88,9
	Continu (24/7)	6	11,1	11,1	100,0
	Total	54	100,0	100,0	

Voor welke doeleinden wordt internet binnen uw organisatie gebruikt en hoe vaak? - Surfen (ongericht).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet	8	14,8	14,8	14,8
	Minder dan maandelijks	7	13,0	13,0	27,8
	Maandelijks	3	5,6	5,6	33,3
	Wekelijks	13	24,1	24,1	57,4
	Dagelijks	20	37,0	37,0	94,4
	Continu (24/7)	3	5,6	5,6	100,0
	Total	54	100,0	100,0	

Voor welke doeleinden wordt internet binnen uw organisatie gebruikt en hoe vaak? - Internetbankieren.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet	7	13,0	13,0	13,0
	Maandelijks	5	9,3	9,3	22,2
	Wekelijks	19	35,2	35,2	57,4
	Dagelijks	21	38,9	38,9	96,3
	Continu (24/7)	2	3,7	3,7	100,0
	Total	54	100,0	100,0	

Voor welke doeleinden wordt internet binnen uw organisatie gebruikt en hoe vaak? - Online boekhouding.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet	12	22,2	22,2	22,2
	Minder dan maandelijks	1	1,9	1,9	24,1
	Maandelijks	5	9,3	9,3	33,3
	Wekelijks	15	27,8	27,8	61,1
	Dagelijks	19	35,2	35,2	96,3
	Continu (24/7)	2	3,7	3,7	100,0
	Total	54	100,0	100,0	

Voor welke doeleinden wordt internet binnen uw organisatie gebruikt en hoe vaak? - Downloaden van muziek, films, en/of software.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet	28	51,9	51,9	51,9
	Minder dan maandelijks	11	20,4	20,4	72,2
	Maandelijks	7	13,0	13,0	85,2
	Wekelijks	5	9,3	9,3	94,4
	Dagelijks	3	5,6	5,6	100,0
	Total	54	100,0	100,0	

Voor welke doeleinden wordt internet binnen uw organisatie gebruikt en hoe vaak? - Beeldbellen: teleconferencing bijvoorbeeld via Skype.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet	30	55,6	55,6	55,6
	Minder dan maandelijks	12	22,2	22,2	77,8
	Maandelijks	7	13,0	13,0	90,7
	Wekelijks	4	7,4	7,4	98,1
	Continu (24/7)	1	1,9	1,9	100,0
	Total	54	100,0	100,0	

Voor welke doeleinden wordt internet binnen uw organisatie gebruikt en hoe vaak? - Chatten (tekstueel).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet	21	38,9	38,9	38,9
	Minder dan maandelijks	8	14,8	14,8	53,7
	Maandelijks	3	5,6	5,6	59,3
	Wekelijks	12	22,2	22,2	81,5
	Dagelijks	8	14,8	14,8	96,3
	Continu (24/7)	2	3,7	3,7	100,0
	Total	54	100,0	100,0	

Question 10

Maakt uw organisatie gebruik van social media?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee.	6	11,1	11,1	11,1
	Ja.	48	88,9	88,9	100,0
	Total	54	100,0	100,0	

Question 11

Hoe vaak maakt uw organisatie gebruik van de volgende social media? - Twitter.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet	37	68,5	68,5	68,5
	Minder dan maandelijks	3	5,6	5,6	74,1
	Maandelijks	2	3,7	3,7	77,8
	Wekelijks	4	7,4	7,4	85,2
	Dagelijks	8	14,8	14,8	100,0
	Total	54	100,0	100,0	

Hoe vaak maakt uw organisatie gebruik van de volgende social media? - Facebook.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet	12	22,2	22,2	22,2
	Minder dan maandelijks	7	13,0	13,0	35,2
	Maandelijks	2	3,7	3,7	38,9
	Wekelijks	16	29,6	29,6	68,5
	Dagelijks	16	29,6	29,6	98,1
	Continu (24/7)	1	1,9	1,9	100,0
	Total	54	100,0	100,0	

Hoe vaak maakt uw organisatie gebruik van de volgende social media? - Instagram.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet	26	48,1	48,1	48,1
	Minder dan maandelijks	3	5,6	5,6	53,7
	Maandelijks	3	5,6	5,6	59,3
	Wekelijks	10	18,5	18,5	77,8
	Dagelijks	12	22,2	22,2	100,0
	Total	54	100,0	100,0	

Hoe vaak maakt uw organisatie gebruik van de volgende social media? - LinkedIn.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet	16	29,6	29,6	29,6
	Minder dan maandelijks	4	7,4	7,4	37,0
	Maandelijks	8	14,8	14,8	51,9
	Wekelijks	17	31,5	31,5	83,3
	Dagelijks	8	14,8	14,8	98,1
	Continu (24/7)	1	1,9	1,9	100,0
	Total	54	100,0	100,0	

Hoe vaak maakt uw organisatie gebruik van de volgende social media? - Videosites zoals YouTube.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet	35	64,8	64,8	64,8
	Minder dan maandelijks	6	11,1	11,1	75,9
	Maandelijks	6	11,1	11,1	87,0
	Wekelijks	7	13,0	13,0	100,0
	Total	54	100,0	100,0	

Hoe vaak maakt uw organisatie gebruik van de volgende social media? - Een (discussie)forum.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet	39	72,2	72,2	72,2
	Minder dan maandelijks	8	14,8	14,8	87,0
	Maandelijks	3	5,6	5,6	92,6
	Wekelijks	2	3,7	3,7	96,3
	Dagelijks	1	1,9	1,9	98,1
	Continu (24/7)	1	1,9	1,9	100,0
	Total	54	100,0	100,0	

Hoe vaak maakt uw organisatie gebruik van de volgende social media? - Een blog.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet	35	64,8	64,8	64,8
	Minder dan maandelijks	8	14,8	14,8	79,6
	Maandelijks	8	14,8	14,8	94,4
	Wekelijks	2	3,7	3,7	98,1
	Dagelijks	1	1,9	1,9	100,0
	Total	54	100,0	100,0	

Question 12

In hoeverre bent u op de hoogte van de online beveiliging van het bedrijf?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet.	8	14,8	14,8	14,8
	In kleine mate.	16	29,6	29,6	44,4
	In grote mate.	7	13,0	13,0	57,4
	Volledig.	2	3,7	3,7	61,1
	Niet in kleine mate, maar ook niet in grote mate.	21	38,9	38,9	100,0
	Total	54	100,0	100,0	

Question 13

In welke mate houdt u zich bezig het voorkomen van cybercrime binnen uw organisatie?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet.	24	44,4	44,4	44,4
	In kleine mate.	13	24,1	24,1	68,5
	Niet in kleine mate, maar ook niet in grote mate.	13	24,1	24,1	92,6
	In grote mate.	3	5,6	5,6	98,1
	Volledig.	1	1,9	1,9	100,0
	Total	54	100,0	100,0	

Question 14

Hoe afhankelijk is uw organisatie van computers en internet (ICT)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet.	3	5,6	5,6	5,6
	In kleine mate.	4	7,4	7,4	13,0
	Niet afhankelijk, maar ook niet onafhankelijk.	8	14,8	14,8	27,8
	In grote mate.	22	40,7	40,7	68,5
	Volledig.	17	31,5	31,5	100,0
	Total	54	100,0	100,0	

Question 15

In welke mate staat op het bedrijfsnetwerk (of op de computers) van uw organisatie vertrouwelijke informatie opgeslagen, zoals klant-, administratiegegevens en/of informatie over productontwikkeling?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet.	7	13,0	13,0	13,0
	In kleine mate.	8	14,8	14,8	27,8
	Niet in kleine mate, maar ook niet in grote mate.	6	11,1	11,1	38,9
	In grote mate.	15	27,8	27,8	66,7
	In zeer grote mate.	18	33,3	33,3	100,0
	Total	54	100,0	100,0	

Question 16

In welke mate bent u bekend met de online veiligheidsrisico's die uw organisatie loopt?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet.	10	18,5	18,5	18,5
	In kleine mate.	16	29,6	29,6	48,1
	Niet in kleine mate, maar ook niet in grote mate.	15	27,8	27,8	75,9
	In grote mate.	9	16,7	16,7	92,6
	In zeer grote mate.	4	7,4	7,4	100,0
	Total	54	100,0	100,0	

Question 17

Hoe belangrijk is het beveiligen van digitale, bedrijfsgerelateerde informatie voor uw organisatie?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Heel onbelangrijk.	1	1,9	1,9	1,9
	Onbelangrijk.	4	7,4	7,4	9,3
	Niet onbelangrijk, maar ook niet belangrijk.	8	14,8	14,8	24,1
	Belangrijk.	22	40,7	40,7	64,8
	Heel belangrijk.	19	35,2	35,2	100,0
	Total	54	100,0	100,0	

Question 18

Welke fysieke maatregelen heeft uw organisatie genomen om online risico's (zoveel mogelijk) uit te sluiten? - ICT, zoals computers en servers, is voorzien van een identificatiekenmerk waarmee kan worden achterhaald of deze toebehoort aan het bedrijf (bijvoorbeeld d.m.v. een postcode of inloggegevens).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	16	29,6	29,6	29,6
	Ja	20	37,0	37,0	66,7
	Weet ik niet	18	33,3	33,3	100,0
	Total	54	100,0	100,0	

Welke fysieke maatregelen heeft uw organisatie genomen om online risico's (zoveel mogelijk) uit te sluiten? - Computers en/of laptops zijn bevestigd aan een kabel.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	30	55,6	55,6	55,6
	Ja	20	37,0	37,0	92,6
	Weet ik niet	4	7,4	7,4	100,0
	Total	54	100,0	100,0	

Question 19

Welke technische maatregelen heeft uw organisatie genomen om online risico's zoveel mogelijk uit te sluiten? - De computers van de organisatie zijn voorzien van een virus scanner.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	4	7,4	7,4	7,4
	Ja	46	85,2	85,2	92,6
	Weet ik niet	4	7,4	7,4	100,0
	Total	54	100,0	100,0	

Welke technische maatregelen heeft uw organisatie genomen om online risico's zoveel mogelijk uit te sluiten? - De computers en/of het netwerk van de organisatie zijn/is voorzien van een firewall.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	2	3,7	3,7	3,7
	Ja	44	81,5	81,5	85,2
	Weet ik niet	8	14,8	14,8	100,0
	Total	54	100,0	100,0	

Welke technische maatregelen heeft uw organisatie genomen om online risico's zoveel mogelijk uit te sluiten? - Het (draadloze) netwerk is beveiligd.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	1	1,9	1,9	1,9
	Ja	49	90,7	90,7	92,6
	Weet ik niet	4	7,4	7,4	100,0
	Total	54	100,0	100,0	

Welke technische maatregelen heeft uw organisatie genomen om online risico's zoveel mogelijk uit te sluiten? - De software op het bedrijfsnetwerk wordt up-to-date gehouden.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	2	3,7	3,7	3,7
	Ja	45	83,3	83,3	87,0
	Weet ik niet	7	13,0	13,0	100,0
	Total	54	100,0	100,0	

Welke technische maatregelen heeft uw organisatie genomen om online risico's zoveel mogelijk uit te sluiten? - (Internet)activiteiten op het bedrijfsnetwerk worden geregistreerd (gelogd*).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	12	22,2	22,2	22,2
	Ja	22	40,7	40,7	63,0
	Weet ik niet	20	37,0	37,0	100,0
	Total	54	100,0	100,0	

Welke technische maatregelen heeft uw organisatie genomen om online risico's zoveel mogelijk uit te sluiten? - *De logs worden (regelmatig) bekeken/geëvalueerd.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	17	31,5	31,5	31,5
	Ja	14	25,9	25,9	57,4
	Weet ik niet	23	42,6	42,6	100,0
	Total	54	100,0	100,0	

Welke technische maatregelen heeft uw organisatie genomen om online risico's zoveel mogelijk uit te sluiten? - Er worden regelmatig back-ups gemaakt van bestanden op computers en/of het bedrijfsnetwerk.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	6	11,1	11,1	11,1
	Ja	41	75,9	75,9	87,0
	Weet ik niet	7	13,0	13,0	100,0
	Total	54	100,0	100,0	

Question 20

Welke beleidsmaatregelen heeft uw organisatie genomen om online risico's (zoveel mogelijk) uit te sluiten? - Er is een protocol opgesteld waarin is beschreven hoe te handelen bij cybercrime.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	37	68,5	68,5	68,5
	Ja	4	7,4	7,4	75,9
	Weet niet	13	24,1	24,1	100,0
	Total	54	100,0	100,0	

Welke beleidsmaatregelen heeft uw organisatie genomen om online risico's (zoveel mogelijk) uit te sluiten? - Er is informatiebeveiligingsbeleid aanwezig (Bijvoorbeeld, regels m.b.t melding en registratie, behandeling van media, uitwisseling van informatie, beveiliging van personeel en fysieke bedrijfsbeveiliging).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	29	53,7	53,7	53,7
	Ja	14	25,9	25,9	79,6
	Weet niet	11	20,4	20,4	100,0
	Total	54	100,0	100,0	

Welke beleidsmaatregelen heeft uw organisatie genomen om online risico's (zoveel mogelijk) uit te sluiten? - Werknemers worden bewust gemaakt van online risico's.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	26	48,1	48,1	48,1
	Ja	25	46,3	46,3	94,4
	Weet niet	3	5,6	5,6	100,0
	Total	54	100,0	100,0	

Welke beleidsmaatregelen heeft uw organisatie genomen om online risico's (zoveel mogelijk) uit te sluiten? - Er zijn regels op schrift gesteld over het gebruik van ICT voor privé-doeleinden.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	39	72,2	72,2	72,2
	Ja	8	14,8	14,8	87,0
	Weet niet	7	13,0	13,0	100,0
	Total	54	100,0	100,0	

Welke beleidsmaatregelen heeft uw organisatie genomen om online risico's (zoveel mogelijk) uit te sluiten? - Er zijn regels op schrift gesteld voor het doen van online betalingen.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	42	77,8	77,8	77,8
	Ja	5	9,3	9,3	87,0
	Weet niet	7	13,0	13,0	100,0
	Total	54	100,0	100,0	

Welke beleidsmaatregelen heeft uw organisatie genomen om online risico's (zoveel mogelijk) uit te sluiten? - Er zijn regels op schrift gesteld over het omgaan met vertrouwelijke informatie, zoals persoonsgegevens van u, uw medewerkers en/of klanten.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	20	37,0	37,0	37,0
	Ja	33	61,1	61,1	98,1
	Weet niet	1	1,9	1,9	100,0
	Total	54	100,0	100,0	

Welke beleidsmaatregelen heeft uw organisatie genomen om online risico's (zoveel mogelijk) uit te sluiten? - Er zijn regels op schrift gesteld over het openen van onbekende bestanden (zoals bijlagen in e-mails).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	32	59,3	59,3	59,3
	Ja	17	31,5	31,5	90,7
	Weet niet	5	9,3	9,3	100,0
	Total	54	100,0	100,0	

Welke beleidsmaatregelen heeft uw organisatie genomen om online risico's (zoveel mogelijk) uit te sluiten? - Er zijn regels op schrift gesteld over het (op verzoek) afgeven van bedrijfsgegevens.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	27	50,0	50,0	50,0
	Ja	24	44,4	44,4	94,4
	Weet niet	3	5,6	5,6	100,0
	Total	54	100,0	100,0	

Welke beleidsmaatregelen heeft uw organisatie genomen om online risico's (zoveel mogelijk) uit te sluiten? - Er worden regelmatig (veiligheid)controles uitgevoerd.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	29	53,7	53,7	53,7
	Ja	18	33,3	33,3	87,0
	Weet niet	7	13,0	13,0	100,0
	Total	54	100,0	100,0	

Question 21

Hoeveel vertrouwen heeft u in het totaal van de door de organisatie genomen maatregelen om cybercrime (online risico's) te voorkomen?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Heel weinig vertrouwen.	3	5,6	5,6	5,6
	Weinig vertrouwen.	4	7,4	7,4	13,0
	Niet weinig en niet veel vertrouwen.	25	46,3	46,3	59,3
	Veel vertrouwen.	17	31,5	31,5	90,7
	Heel veel vertrouwen.	5	9,3	9,3	100,0
	Total	54	100,0	100,0	

Question 22

Hoe tevreden bent u met de in totaal door de organisatie genomen maatregelen om cybercrime te voorkomen?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Heel ontevreden.	1	1,9	1,9	1,9
	Ontevreden.	2	3,7	3,7	5,6
	Niet ontevreden, niet tevreden.	26	48,1	48,1	53,7
	Tevreden.	21	38,9	38,9	92,6
	Heel tevreden.	4	7,4	7,4	100,0
	Total	54	100,0	100,0	

Question 23

Zou uw organisatie meer maatregelen moeten nemen om cybercrime te voorkomen?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee.	15	27,8	27,8	27,8
	Ja.	16	29,6	29,6	57,4
	Weet ik niet.	23	42,6	42,6	100,0
	Total	54	100,0	100,0	

Question 24

Is uw organisatie wel eens slachtoffer geworden van cybercrime?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee, de organisatie is geen slachtoffer van cybercrime geworden.	40	74,1	74,1	74,1
	Ja, in de afgelopen twaalf maanden.	2	3,7	3,7	77,8
	Ja, meer dan een jaar geleden.	4	7,4	7,4	85,2
	Weet ik niet.	8	14,8	14,8	100,0
	Total	54	100,0	100,0	

Question 25

In hoeverre heeft uw organisatie in de afgelopen twaalf maanden te maken gehad met de volgend criminaliteitsvormen - Afpersing via internet (het moeten betalen van geld of goederen door bedreiging en/of geweld.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet mee te maken gehad	47	87,0	87,0	87,0
	Weet niet	4	7,4	7,4	94,4
	Eén keer slachtoffer	3	5,6	5,6	100,0
	Total	54	100,0	100,0	

In hoeverre heeft uw organisatie in de afgelopen twaalf maanden te maken gehad met de volgend criminaliteitsvormen - Chantage via internet (het moeten afgeven van geld of goederen door te dreigen met het openbaar maken van een geheim of smaadschrift.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Eén of meerdere mislukte pogingen	1	1,9	1,9	1,9
	Niet mee te maken gehad	50	92,6	92,6	94,4
	Weet niet	3	5,6	5,6	100,0
	Total	54	100,0	100,0	

In hoeverre heeft uw organisatie in de afgelopen twaalf maanden te maken gehad met de volgend criminaliteitsvormen - Denial of Service (DoS-) aanval (digitale aanvallen op het systeem waardoo deze wordt overbelast en niet meer beschikbaar is, bijvoorbeeld het platleggen van een website.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Eén of meerdere mislukte pogingen	2	3,7	3,7	3,7
	Niet mee te maken gehad	48	88,9	88,9	92,6
	Weet niet	4	7,4	7,4	100,0
	Total	54	100,0	100,0	

In hoeverre heeft uw organisatie in de afgelopen twaalf maanden te maken gehad met de volgend criminaliteitsvormen - Defacing (het zonder toestemmen veranderen/bekladden, vervangen of vernielen van de website van uw organisatie).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Eén of meerdere mislukte pogingen	1	1,9	1,9	1,9
	Niet mee te maken gehad	49	90,7	90,7	92,6
	Weet niet	4	7,4	7,4	100,0
	Total	54	100,0	100,0	

In hoeverre heeft uw organisatie in de afgelopen twaalf maanden te maken gehad met de volgend criminaliteitsvormen - Diefstal van datadragers (zoals pc, laptop, usb-sticks)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet mee te maken gehad	49	90,7	90,7	90,7
	Weet niet	3	5,6	5,6	96,3
	Eén keer slachtoffer	2	3,7	3,7	100,0
	Total	54	100,0	100,0	

In hoeverre heeft uw organisatie in de afgelopen twaalf maanden te maken gehad met de volgend criminaliteitsvormen - Diefstal van gegevens (die niet voor de dader bestemd zijn)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet mee te maken gehad	46	85,2	85,2	85,2
	Weet niet	5	9,3	9,3	94,4
	Eén keer slachtoffer	3	5,6	5,6	100,0
	Total	54	100,0	100,0	

In hoeverre heeft uw organisatie in de afgelopen twaalf maanden te maken gehad met de volgend criminaliteitsvormen - Hacking (inbraak op de computersystemen van uw organisatie)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet mee te maken gehad	46	85,2	85,2	85,2
	Weet niet	6	11,1	11,1	96,3
	Eén keer slachtoffer	2	3,7	3,7	100,0
	Total	54	100,0	100,0	

In hoeverre heeft uw organisatie in de afgelopen twaalf maanden te maken gehad met de volgend criminaliteitsvormen - Identiteitsmisbruik (het misbruik maken van de identiteitsgegevens van uw organisatie)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet mee te maken gehad	46	85,2	85,2	85,2
	Weet niet	5	9,3	9,3	94,4
	Eén keer slachtoffer	3	5,6	5,6	100,0
	Total	54	100,0	100,0	

In hoeverre heeft uw organisatie in de afgelopen twaalf maanden te maken gehad met de volgend criminaliteitsvormen - Malware (infectie van computersystemen middels virussen, trojan horses en/of spyware)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Eén of meerdere mislukte pogingen	5	9,3	9,3	9,3
	Niet mee te maken gehad	40	74,1	74,1	83,3
	Weet niet	6	11,1	11,1	94,4
	Eén keer slachtoffer	3	5,6	5,6	100,0
	Total	54	100,0	100,0	

In hoeverre heeft uw organisatie in de afgelopen twaalf maanden te maken gehad met de volgend criminaliteitsvormen - Ongeautoriseerd gebruik van het bedrijfsnetwerk (bijvoorbeeld door middel van het downloaden/verspreiden van illegale software, kinderpornografie, spam of het plaatsen van berichten van racistische of discriminerende aard).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet mee te maken gehad	48	88,9	88,9	88,9
	Weet niet	5	9,3	9,3	98,1
	Eén keer slachtoffer	1	1,9	1,9	100,0
	Total	54	100,0	100,0	

In hoeverre heeft uw organisatie in de afgelopen twaalf maanden te maken gehad met de volgend criminaliteitsvormen - Phishing (het via digitale middelen - email of social media - met een verzinsel informatie over uw bedrijf ontfutselen via mensen binnen uw organisatie.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Eén of meerdere mislukte pogingen	12	22,2	22,2	22,2
	Niet mee te maken gehad	36	66,7	66,7	88,9
	Weet niet	6	11,1	11,1	100,0
	Total	54	100,0	100,0	

In hoeverre heeft uw organisatie in de afgelopen twaalf maanden te maken gehad met de volgend criminaliteitsvormen - Skimming (waarbij op onrechtmatige wijze zijn pinpas- of creditcardgegevens van uw organisatie bemachtigd en gekopieerd).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Eén of meerdere mislukte pogingen	3	5,6	5,6	5,6
	Niet mee te maken gehad	46	85,2	85,2	90,7
	Weet niet	3	5,6	5,6	96,3
	Eén keer slachtoffer	2	3,7	3,7	100,0
	Total	54	100,0	100,0	

In hoeverre heeft uw organisatie in de afgelopen twaalf maanden te maken gehad met de volgend criminaliteitsvormen - Skimming (waarbij daders het pinapparaat van uw organisatie hebben aangepast).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Eén of meerdere mislukte pogingen	1	1,9	1,9	1,9
	Niet mee te maken gehad	50	92,6	92,6	94,4
	Weet niet	3	5,6	5,6	100,0
	Total	54	100,0	100,0	

In hoeverre heeft uw organisatie in de afgelopen twaalf maanden te maken gehad met de volgend criminaliteitsvormen - Smaad/laster via internet (het via ICT opzettelijk aantasten van de goede naam van uw organisatie).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Eén of meerdere mislukte pogingen	2	3,7	3,7	3,7
	Niet mee te maken gehad	44	81,5	81,5	85,2
	Weet niet	6	11,1	11,1	96,3
	Eén keer slachtoffer	1	1,9	1,9	98,1
	Meerdere keren slachtoffer	1	1,9	1,9	100,0
	Total	54	100,0	100,0	

In hoeverre heeft uw organisatie in de afgelopen twaalf maanden te maken gehad met de volgend criminaliteitsvormen - Fraude/oplichting (via internet (financiële) schade opgelopen middels bedrog).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Eén of meerdere mislukte pogingen	2	3,7	3,7	3,7
	Niet mee te maken gehad	46	85,2	85,2	88,9
	Weet niet	4	7,4	7,4	96,3
	Eén keer slachtoffer	2	3,7	3,7	100,0
	Total	54	100,0	100,0	

Question 26 (Multiple answers possible)

Van welke vorm van oplichting/fraude via internet en/of de mobiele telefoon is uw organisatie slachtoffer geworden? (meerdere antwoorden mogelijk) - Selected Choice De organisatie heeft iets gekocht, maar het product/de dienst niet ontvangen.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	De organisatie heeft iets gekocht, maar het product/de dienst niet ontvangen.	1	1,9	100,0	100,0
Missing	System	53	98,1		
Total		54	100,0		

Van welke vorm van oplichting/fraude via internet en/of de mobiele telefoon is uw organisatie slachtoffer geworden? (meerdere antwoorden mogelijk) - Selected Choice Acquisitiefraude en/of spookfacturen: een vorm van oplichting waarbij producten worden aangeboden die geen waarde hebben, of kosten in rekening worden gebracht voor diensten die niet zijn geleverd of waarvoor geen opdracht is gegeven.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Acquisitiefraude en/of spookfacturen: een vorm van oplichting waarbij producten worden aangeboden die geen waarde hebben, of kosten in rekening worden gebracht voor diensten die niet zijn geleverd of waarvoor geen opdracht is gegeven.	1	1,9	100,0	100,0
Missing	System	53	98,1		
Total		54	100,0		

Question 27

Wat is het laatste cybercrime incident dat uw organisatie heeft meegemaakt?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Afpersing.	1	1,9	7,1	7,1
	Diefstal van gegevens.	1	1,9	7,1	14,3
	Fraude/oplichting.	2	3,7	14,3	28,6
	Hacking.	3	5,6	21,4	50,0
	Identiteitsmisbruik.	2	3,7	14,3	64,3
	Malware.	3	5,6	21,4	85,7
	Ongeautoriseerd gebruik van het bedrijfsnetwerk.	1	1,9	7,1	92,9
	Skimming (waarbij op onrechtmatige wijze de pinpas- of creditcardgegevens van uw organisatie zijn bemachtigd en gekopieerd).	1	1,9	7,1	100,0
	Total	14	25,9	100,0	
Missing	System	40	74,1		
Total		54	100,0		

Question 28

Weet uw organisatie wie deze cybercrime heeft gepleegd?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ja.	3	5,6	21,4	21,4
	Er is een vermoeden.	1	1,9	7,1	28,6
	Nee.	9	16,7	64,3	92,9
	Weet niet.	1	1,9	7,1	100,0
	Total	14	25,9	100,0	
Missing	System	40	74,1		
Total		54	100,0		

Question 29

Wie heeft (vermoedelijk) de cybercrime gepleegd? - Selected Choice

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Een medewerker.	1	1,9	25,0	25,0
	Een klant.	1	1,9	25,0	50,0
	Anders, namelijk...	2	3,7	50,0	100,0
	Total	4	7,4	100,0	
Missing	System	50	92,6		
Total		54	100,0		

1. Iemand die iets probeert te verkopen onder onze naam.
2. Er is niets gebeurd, dat kon ik alleen twee vragen terug niet aanvinken om verder te komen in de enquête.

Question 30

Welke schade heeft uw organisatie in het afgelopen jaar (2017) ondervonden van cybercrime? - Selected Choice

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Geen schade.	9	16,7	64,3	64,3
	Financiële schade.	2	3,7	14,3	78,6
	Verlies en/of beschadiging van gegevens.	1	1,9	7,1	85,7
	Schade in de vorm van tijdverlies.	1	1,9	7,1	92,9
	Anders, namelijk...	1	1,9	7,1	100,0
	Total	14	25,9	100,0	
Missing	System	40	74,1		
Total		54	100,0		

Question 31

Hoe groot was de financiële schade (ongeveer)? Afronden op hele bedragen. - Selected Choice

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Euro	1	1,9	50,0	50,0
	Weet ik niet.	1	1,9	50,0	100,0
	Total	2	3,7	100,0	
Missing	System	52	96,3		
Total		54	100,0		

1. 2500 euro

Question 32 (Multiple answers possible)

Statistics

		Welke actie (s) heeft uw organisatie ondernomen na het constateren van de betreffende cybercrime? (meerdere antwoorden mogelijk) - Selected Choice Geen.	Welke actie (s) heeft uw organisatie ondernomen na het constateren van de betreffende cybercrime? (meerdere antwoorden mogelijk) - Selected Choice Mijn organisatie heeft zichzelf geprobeerd schadeloos te stellen / is schadeloos gesteld: de schade is bijvoorbeeld vergoed door een verzekeraar/ bank, de handelsite/webwinkel of de dader heeft de ontvreemde goederen teruggegeven.	Welke actie (s) heeft uw organisatie ondernomen na het constateren van de betreffende cybercrime? (meerdere antwoorden mogelijk) - Selected Choice Mijn organisatie heeft het probleem zelf opgelost, bijvoorbeeld door de eigen IT-afdeling onderzoek uit te laten voeren (de virusinfectie ongedaan maken / het lek dichten).	Welke actie (s) heeft uw organisatie ondernomen na het constateren van de betreffende cybercrime? (meerdere antwoorden mogelijk) - Selected Choice Mijn organisatie heeft een onafhankelijk onderzoeksbureau (privé detective/recherche bureau) ingeschakeld om het probleem op te lossen.	Welke actie (s) heeft uw organisatie ondernomen na het constateren van de betreffende cybercrime? (meerdere antwoorden mogelijk) - Selected Choice Mijn organisatie heeft maatregelen genomen (ervan geleerd) om toekomstig slachtofferschap te voorkomen.	Welke actie (s) heeft uw organisatie ondernomen na het constateren van de betreffende cybercrime? (meerdere antwoorden mogelijk) - Selected Choice Er is contact gezocht met de politie (bijvoorbeeld om melding of aangifte te doen).	Welke actie (s) heeft uw organisatie ondernomen na het constateren van de betreffende cybercrime? (meerdere antwoorden mogelijk) - Selected Choice Er is contact gezocht met een belangenorganisatie (zoals branchevereniging, Kamer van Koophandel, fraudehelpdesk, etc.).	Welke actie (s) heeft uw organisatie ondernomen na het constateren van de betreffende cybercrime? (meerdere antwoorden mogelijk) - Selected Choice Er is een juridische dienstverlener ingeschakeld.	Welke actie (s) heeft uw organisatie ondernomen na het constateren van de betreffende cybercrime? (meerdere antwoorden mogelijk) - Selected Choice Weet niet.	Welke actie (s) heeft uw organisatie ondernomen na het constateren van de betreffende cybercrime? (meerdere antwoorden mogelijk) - Selected Choice Anders, namelijk...
N	Valid	4	1	3	0	3	1	1	0	1	2
	Missing	50	53	51	54	51	53	53	54	53	52

When answered "anders" → 1. De bank is gebeld, 2. Er is niets gebeurd.

Question 33

Met welke belangenorganisatie is contact gezocht nadat uw organisatie slachtoffer is geworden van cybercrime? (Meerdere antwoorden mogelijk) - Selected Choice

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Regionale ondernemersorganisaties en/of brancheorganisaties.	1	1,9	7,1	7,1
	Fraudehelpdesk.	1	1,9	7,1	14,3
	Anders, namelijk...	12	22,2	85,7	100,0
	Total	14	25,9	100,0	
Missing	System	40	74,1		
Total		54	100,0		

Question 34

Indien uw organisatie in de toekomst slachtoffer wordt van cybercrime, zou uw organisatie hiervan dan aangifte bij de politie?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee.	2	3,7	3,7	3,7
	Ja.	36	66,7	66,7	70,4
	Misschien.	16	29,6	29,6	100,0
	Total	54	100,0	100,0	

Question 35 (Multiple answers possible)

Waarom zou uw organisatie hiervan (misschien) geen aangifte doen? (Meerdere antwoorden mogelijk) - Selected Choice Het hangt af van de hoogte van de (financiële) schade.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Het hangt af van de hoogte van de (financiële) schade.	18	33,3	100,0	100,0
Missing	System	36	66,7		
Total		54	100,0		

Waarom zou uw organisatie hiervan (misschien) geen aangifte doen? (Meerdere antwoorden mogelijk) - Selected Choice Dit is geen zaak voor de politie.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Dit is geen zaak voor de politie.	1	1,9	100,0	100,0
Missing	System	53	98,1		
Total		54	100,0		

Waarom zou uw organisatie hiervan (misschien) geen aangifte doen? (Meerdere antwoorden mogelijk) - Selected Choice De politie doet er niets mee.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	De politie doet er niets mee.	7	13,0	100,0	100,0
Missing	System	47	87,0		
Total		54	100,0		

Waarom zou uw organisatie hiervan (misschien) geen aangifte doen? (Meerdere antwoorden mogelijk) - Selected Choice De politie is niet in staat de dader te vinden.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	De politie is niet in staat de dader te vinden.	3	5,6	100,0	100,0
Missing	System	51	94,4		
Total		54	100,0		

Waarom zou uw organisatie hiervan (misschien) geen aangifte doen? (Meerdere antwoorden mogelijk) - Selected Choice Het wordt door de organisatie zelf opgelost.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Het wordt door de organisatie zelf opgelost.	4	7,4	100,0	100,0
Missing	System	50	92,6		
Total		54	100,0		

Waarom zou uw organisatie hiervan (misschien) geen aangifte doen? (Meerdere antwoorden mogelijk) - Selected Choice Dan volgen er misschien represailles (=handelingen uit wraak) van de dader.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Dan volgen er misschien represailles (=handelingen uit wraak) van de dader.	1	1,9	100,0	100,0
Missing	System	53	98,1		
Total		54	100,0		

Waarom zou uw organisatie hiervan (misschien) geen aangifte doen? (Meerdere antwoorden mogelijk) - Selected Choice Dit zorgt mogelijk voor imagoschade.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Dit zorgt mogelijk voor imagoschade.	1	1,9	100,0	100,0
Missing	System	53	98,1		
Total		54	100,0		

Waarom zou uw organisatie hiervan (misschien) geen aangifte doen? (Meerdere antwoorden mogelijk) - Selected Choice Dit kost teveel moeite (tijd/geld).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Dit kost teveel moeite (tijd/geld).	6	11,1	100,0	100,0
Missing	System	48	88,9		
Total		54	100,0		

Waarom zou uw organisatie hiervan (misschien) geen aangifte doen? (Meerdere antwoorden mogelijk) - Selected Choice Weet ik niet.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Weet ik niet.	6	11,1	100,0	100,0
Missing	System	48	88,9		
Total		54	100,0		

Waarom zou uw organisatie hiervan (misschien) geen aangifte doen? (Meerdere antwoorden mogelijk) - Selected Choice Ik zou wel aangifte doen.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ik zou wel aangifte doen.	25	46,3	100,0	100,0
Missing	System	29	53,7		
Total		54	100,0		

Question 36[2]

"Heeft u zelf nog vragen en/of opmerkingen die u wilt benoemen?"

-	Nee	Nee	Veel kan niet online, moet in persoon gebeuren. Dat zet een grote rem op het aangifte doen	Nee	Neen	Geen aanvullingen	Nee
-	Nee	Nee	Nee	Geen	Nee	Nee	Mis af en toe de antwoord-optie; n.v.t.
Nee	Nee	Nee	Nee	Nee	Wij zijn onderdeel van een franchiseorganisatie en op veel vragen kunnen wij geen antwoord geven daar dit geregeld wordt door het hoofdkantoor.	Nee	Nee
Geen	Neen	Nee	Nee	Nee	Nee	Nee geen opmerkingen	Nvt
Nee	Nee	Nee	-	Nee	Geen	Nee	Neen
Nvt	Nee	Nee	Nee	Nee	Nee, geen vragen.	Nee	Ben nu wel alerter door dit onderzoek en zal zeker onderzoek doen.
Geen	Nee	Nee	Nee	Vraag q33 is niet juist beantwoord omdat deze vraag beantwoord moet worden en nooit heeft plaatsgevonden. Antwoord als bv 'niet van toepassing' zou ook een keuze moeten zijn!	Werd na melding goed behandeld		

Question 37

Bent u hier gekomen via MKB Twente?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee.	50	92,6	92,6	92,6
	Ja.	4	7,4	7,4	100,0
	Total	54	100,0	100,0	

[2] For better readability, stylistics and linguistic errors, in the answers given at question 36, have been corrected.

Appendix VI: Tables.

Table 1

Vraag 9: voor welke doeleinden wordt internet binnen uw organisatie gebruikt en hoe vaak? (n=54)

	Not at all	Less than monthly	Monthly	Weekly	Daily	Continuous; 24/7
Placing orders	27,8%	9,3%	16,7%	20,4%	20,4	5,6%
Email	3,7%			7,4%	63%	25,9%
Searching for information (aimed)	1,9%		5,6%	16,7%	64,8%	11,1%
Surfing (un-aimed)	14,8%	13%	5,6%	24,1%	37%	5,6%
Internet banking	13%		9,3%	35,2%	38,9%	3,7%
Online financing	22,2%	1,9%	9,3%	27,8%	35,2%	3,7%
Downloading of music, films and/or software	51,9%	20,4%	13%	9,3%	5,6%	
Teleconferencing	55,6%	22,2%	13%	7,4%		1,9%
Chatting (text)	38,9%	14,8	5,6%	22,2%	14,8%	3,7%

Table 2

Vraag 11: hoe vaak maakt uw organisatie gebruik van de volgende social media? (n=54)

	Not at all	Less than monthly	Monthly	Weekly	Daily	Continuous; 24/7
Twitter	68,5%	5,6%	3,7%	7,4%	14,8%	
Facebook	22,2%	13%	3,7%	29,6%	29,6%	1,9%
Instagram	48,1%	5,6%	5,6%	18,5%	22,2%	
LinkedIn	29,6%	7,4%	14,8%	31,5%	14,8%	1,9%
Videosites like YouTube	64,8%	11,1%	11,1%	13%		
An Internet forum	72,2%	14,8%	5,6%	3,7%	1,9%	1,9%
A blog	64,8%	14,8%	14,8%	3,7%	1,9%	

Table 3

Vraag 19: welke technische maatregelen heeft uw organisatie genomen om online risico's zoveel mogelijk uit te sluiten? (n=54)

	Yes	No	I do not know
Virus scanner.	85,2%	7,4%	7,4%
Firewall.	81,5%	3,7%	14,8%
The wireless network is protected.	90,7%	1,9%	7,4%
The software is being kept up to date.	83,3%	3,7%	13%
Internet activities are being logged*.	40,7%	22,2%	37%
***These logs are regularly being evaluated.**	25,9%	31,5%	42,6%
Back-ups are being made regularly.	75,9%	11,1%	13%

Table 4

Vraag 20: welke beleidsmaatregelen heeft uw organisatie genomen om online risico's (zoveel mogelijk) uit te sluiten? (n=54)

	Yes	No	I do not know
Protocol that describes how to act when cybercrime happens.	7,4%	68,5%	24,1%
Information security policy.	25,9%	53,7%	20,4%
Employees are being made aware of online risks.	46,3%	48,1%	5,6%
Written rules about the use of ICT for private matters.	14,8%	72,2%	13%
Written rules about making online payments.	9,3%	77,8%	13%
Written rules about how to act with private and confidential information.	61,1%	37%	1,9%
Written rules about how to act with unknown files.	31,5%	59,3%	9,3%
Written rules about transferring business information (at request).	44,4%	50%	5,6%
Safety checks are being executed regularly.	33,3%	53,7%	13%

Table 5

Vraag 25: in hoeverre heeft uw organisatie in de afgelopen twaalf maanden te maken gehad met de volgend criminaliteitsvormen? (n=54)

	I do not know	Not at all	1 or more failed attempts	Once a victim	More than once victim
Extortion	7,4%	87%		5,6%	
Blackmail	5,6%	92,6%	1,9%		
DDos attack	7,4%	88,9%	3,7%		
Defacing	7,4%	90,7%	1,9%		
Theft of data carriers	5,6%	90,7%		3,7%	
Theft of data	9,3%	85,2%		5,6%	
Hacking	11,1%	85,2%		3,7%	
Identity theft	9,3%	85,2%		5,6%	
Malware	11,1%	74,1%	9,3%	5,6%	
Unauthorized use of the organizational network	9,3%	88,9%		1,9%	
Phishing	11,1%	66,7%	22,2%		
Skimming (where debit card or credit card data is being copied)	5,6%	85,2%	5,6%	3,7%	
Skimming (where the pin device is adjusted)	5,6%	92,6%	1,9%		
Defamation, slander and libel	3,7%	81,5%	11,1%	1,9%	1,9%
Fraud/scam	7,4%	85,2%	3,7%	3,7%	

Table 7

Question 32: welke actie(s) heeft uw organisatie ondernomen na het constateren van de betreffende cybercrime? (n=14, meerdere antwoorden mogelijk)

None	The organization tried to compensate via insurance/bank	The organization solved the problem itself	Independent research agency	The organization took safety measures, trying to prevent future victimization	The organization contacted the police	Made contact with an interest group	I do not know	Other
28,5%	7,1%	21,4%		21,4%	7,1%	7,1%	7,1%	14,3%