How to improve cybercrime prevention protocols against ransomware attacks within Dutch municipalities?

Faraj, Bawan

Master's thesis

Cyber Crime prevention within Dutch municipalities

Bawan Faraj (s2781174)

International and European Governance Track

Leiden University

9-1-2022

Word count: 19393

''How to improve cybercrime prevention protocols against ransomware attacks within Dutch municipalities?''

Universiteit Leiden

Preface

Hereby I present my thesis:

''How to improve cybercrime prevention protocols against ransomware attacks within Dutch municipalities?''

This thesis was written to conclude my study at the University Leiden. I have used knowledge that I have learnt during my studies. In addition, I have also used the knowledge that I already had regarding this subject. This is a subject that has fascinated me for years. Of course, during the course of this study, I delved further into it and made sure that I was able to broaden my level of knowledge.

I would like to thank my supervisor, fellow students and family for their trust and support during this process. I was extremely reluctant to take this route and went through deep dumps before I could see the end goal. Once I had this insight, I bit down on my final goal. Besides the fact that I find this an interesting subject, I also think that this is a subject that contributes to a social issue. Integrity issues are coming up more and more often. I therefore hope that this research will provide new insights.

Enjoy reading!

Bawan Faraj

The Hague, 2022

Abstract

This thesis deals with the concept of cybercrime prevention protocols against ransomware attacks within Dutch municipalities. It starts with a description of the development of cybercrime attacks, and ransomware in particular, aimed at Dutch municipalities. Then it follows up with the routine activity theory and current ransomware prevention methods and measurements. The practical part analyses input from employers of municipalities and IT-experts. They provide access to questions asked for the purpose of this investigation. The response is based on experience and successful attacks by hackers on municipalities. After the input has been analysed, a set of recommendations will also be made. These recommendations will be used to improve cybercrime prevention. Conclusively, the consequences of cybercrime prevention protocols on ransomware attacks will also be discussed both in terms of image and financial effect of such protocols.

Key Words:

Cybercrime, cybercrime prevention, protocols, ransomware, Dutch municipalities

Executive summary

More than a fifth of data breach reports in The Netherlands came from the government, including municipalities. Proportionally, this is still low as almost half of all ransomware attacks globally have been targeted at municipalities. However, this indicates that this could be a growing problem in the Netherlands. Municipalities are an area of focus due to high chances of ransom being paid.

Ransomware has been defined as a form of malware that subverts cyber-security mechanisms such as cryptography in order to access and hijack user data. It has been defined in terms of a malicious software which infects computer systems through encryption and thereafter, restricting user access to files and data on the computer till a 'ransom' is paid.

Although it would be assumed that this red flag should lead to measurements and preparedness, none of this is the case. Due to budget constraints, ignorance of not realizing the need of cybercrime prevention protocols nor the possible risks of lacking such measures, are among the reasons most municipalities in Netherlands remain vulnerable systems of cybercrime attacks. Currently there is insufficient research regarding possible faults within the cyber security of Dutch municipalities with regards to ransomware attacks. Therefore, this thesis will be focused on exploring different methods of optimizing cybersecurity in order to stop or at least slow down the increasing rate of cybercrime and more specifically ransomware attacks within Dutch municipalities. Therefore, the main research question is: *''How to improve cybercrime prevention protocols against ransomware attacks within Dutch municipalities?''*

According to routine activity theory, for a crime to occur, there must be three elements. There must be a motivated offender, an appropriate target and lack of a competent guardian. This research uses a qualitative method during which current and former employees who worked within this branch and are known as experts were approached and interviewed. Additionally, specialists on cybersecurity were also approached for an interview due to their specific knowledge on the subject. The respondents work for various municipalities in Netherlands and have at least one year of experience within their respective organisations.

It has emerged that municipalities in the Netherlands have different budgets depending on their size, the number of citizens each municipality holds, , the age of the citizens and the number of citizens receiving benefits. These budgets are subsidized by the central government through municipal funds. The municipalities are free in spending the budget as they see fit as long as they can justify the expenses to the government. This also means that municipalities are not bound by any specific set of guidelines or policies when establishing their own cybersecurity laws against cybercrime and more specifically ransomware. These cybersecurity laws can be made as long as the municipalities follow the requirements set by the Baseline Informatiebeveiliging Overheid (BIO) . These requirements include the security

software or systems they decide to use, which security supplier they decide to work with and also what sort of risk management they want to employ . Another obstacle which is preventing municipalities from improving their chances against ransomware attacks is the existence of a bureaucratic hierarchy within organizations. Ransomware attacks can occur fast and in rapid succession, the time required to react to such an attack if the systems fail is often very little. The administrative culture within the municipality will have to adjust to the situation in order to implement changes more easily in accordance with the situation. Moreover, due to the varying budgets per municipality , the funding put towards cyber-security in Dutch municipalities will also vary.

The municipality of Hof van Twente for example has a yearly budget of 12 million euro´s which is meant to cover the municipality´s expenses on several different areas including cybersecurity. During their ransomware attack, the municipality spent a total of 1.58 million euro´s in costs to mitigate the crisis. After the ransomware attack however, an additional 2.32 million euro´s had been used in order to rebuild the breached systems, which comes down to a financial loss of 4 million euros. Besides the financial loss, such attacks also costs time and creates a delay in the workflow.

Cybercrime prevention can be improved by using a set of actions. These actions either complement each other or contribute separately to the bigger picture. It is important to have various mechanisms in place that actually detect, and monitor everything that happens in that network. In addition, protecting the municipality involves a combination of various components, a so-called life cycle, clear policy, increasing safe and aware behaviour among employees, taking technical measures such as end-point protection for anti-virus and anti-malware on systems, as well as mapping out risks and vulnerabilities.

It is important that the municipality makes its staff aware of cybercrime and ransomware. Municipalities have a unanimous strategy that they will not incur any costs in case such an attack occurs. Despite a lack of a central policy, all municipalities share the same approach. It is precisely the lack of a central policy that is striking and should be a point of attention. Entering a joint venture between municipalities can ensure that software systems are purchased centrally and that similar structures are used. In this way, the SIEM SOC methodology could be deployed more broadly, for example, regional or provincial monitoring could take place during which there is close contact with the IT experts of the municipality in question.

After all, there are municipalities that have smaller budgets and cannot afford to spend a substantial part on cybercrime prevention. It is precisely by sharing the costs (by ratio) associated with cybercrime prevention that many municipalities can comply with security measures. Measures can also be taken within the municipalities themselves.

Two-factor authentication is an example of this. By making this compulsory and using it within all applications, the chance of attacks will be reduced. Not all municipalities have applied it within all

applications, which means that there are still openings for hackers to make use of it. Rules must be created for a password such as the use of upper- and lower-case letters, numbers, and special characters. In addition, the use of network segmentation is recommended whereby a network is divided into different segments. This therefore makes it possible to identify irregularities more easily and timely.

Table of contents

Introduction

Background

The Dutch Data Protection Authority (AP) received 23,976 data breach reports in 2020, out of these, more than a fifth of this figure came from the Dutch government, including municipalities (Authoriteit Persoonsgegevens, 2021). That is an increase of 13 percent compared to 2020. In the past 5 years there has been an increase of data breach reports of about 500%. Moreover, the AP also measured an "explosive increase in the number of hacks" and decided to sound the alarm by sending a data breach report of 2020 to the Second Chamber in order for them to see the urgency of the issue (Authoriteit Persoonsgegevens, 2021a).

Once within the Second Chamber, Kuiken who is a member of the PVDA party decided to ask Minister of Legal protection, Dekker, about the report. Kuiken asked Minister Dekker if he shared the same opinion regarding the alarming hacking, phishing and malware cases that have been reported for the second year in a row (Tweede Kamer der Staten-Generaal, 2021). To which Dekker replied ‘’Recorded cybercrime (including hacking) and digitized crime (including online fraud and babble tricks) have both increased in recent years. Since the beginning of the corona virus crisis, these forms of crime have continued to increase. This is worrisome and it is not known in how many cases personal data has been retrieved or tampered with’’ (Tweede Kamer der Staten-Generaal, 2021).

Within the public sector, the government is not attacked to any great extent (Groenhuijsen, 2020). However, the government still stores very important files such as personal data and valuable information and because of the highly valuable information, the risk of cybercrime is very high (Lovan and Lovan, 2016, p.430). Additionally, the government and more specifically local governments such as municipalities can have reputation damage once any leaks are made public. Moreover, with the public sector’s security not being updated fast enough, the Dutch local governments cannot seem to keep up with the cybercrime cases (Centraal Planbureau, 2019, p.17). However, the slow process of updates does not mean that all organizations within the public sector deal with this same issue, as there are numerous organizations that are doing considerably better with regards to cybercrime prevention.

Because of the lockdowns brought about by the viral corona virus situation in the Netherlands, citizens were spending more time within their homes and exchanging information to continue their daily operations (Van de Laar, 2021; Stil, 2020). The countrywide lockdown made it easier for cybercriminals to engage in criminal activities due to more activity within the digital realm, and therefore gave them a leeway to access even more vulnerable targets (Van der Wiele, 2020). For example, hackers have recently stolen data from IT-supplier Abiom, which works for Defence, the National Police and the Ministry of Justice and Security in the Netherlands (RTL, 2021). The hackers demanded a ransom for the stolen information. The stolen data contained internal documents, including sensitive and confidential

information between governments. Examples of these documents are personal details of executives, copies of passports and various agreements with foreign and local governments, and more specifically municipalities.

Previous empirical studies such as Connolly et al. (2020, p.3) have found that ransomware is the most used method to target municipalities' security systems, which can lead to disruptions in daily operations as a result of systems being taken over. According to research conducted by Fleming Shi (2020), a Chief Technology Officer at Barracuda Networks, almost half of all ransomware attacks globally have been targeted at municipalities. Moreover, Shi (2020) points out that municipalities are undoubtedly an area of focus due to high chances of ransom being paid. Of the studied municipalities, 15 percent have confirmed to have made payments (ransom) to cyber criminals.

Due to the rapid pace at which cybercrime is developing, innovation in software security needs to keep up with this change in order to deal with future challenges (Choi et al., 2020). Although it would be assumed that this red flag should lead to measurements and preparedness, none of this is the case. Due to budget constraints, ignorance of not recognizing the need, and possible risks associated with not having cybercrime protection protocols, most of the Dutch municipalities remain vulnerable to cyber-attacks.

Municipalities in the Netherlands, however, have a strong need for new insights within this issue (Nauta & Wheel, 2021). They would like to know how they can prevent ransomware attacks and which measures they can take to minimize the risk of being targeted. By having this insight, their business operations are able to flow more fluidly without security concerns.

Research Question

Currently insufficient research has taken place which investigates the possible faults within the cyber security system of the Dutch municipalities, with regards to ransomware attacks. Therefore, this thesis is focussed on exploring different proctocols to optimize cybersecurity in order to stop or at least slow down the increasing rate of cybercrime and more specifically ransomware attacks within Dutch municipalities.

Therefore, the main research question is:

''How can Dutch municipalities improve their cybercrime prevention protocols against ransomware attacks?''

A break down in the form of sub questions will lead to answering the main research question.

- *How is cybercrime prevention against ransomware currently configured within municipalities in the Netherlands?*
- *What is preventing municipalities from improving their chances against ransomware attacks?*
- *What sort of change would have to occur in order for municipalities to manage ransomware attacks more effectively?*
- *What are the costs and benefits of improved cybercrime prevention?*

Relevance

This research makes a scientific contribution to the potential risks that municipalities in the Netherlands may currently face. The information resulting from this research could be applied to municipalities where there is a vulnerable landscape within the security systems. An improvement in this area could enable municipalities to be more resistant to possible attacks by hackers in the form of ransomware (Tyagi, 2017, p. 40) The sensitive information could fall into the wrong hands, which is why it is important to provide insight into the current situation where municipalities are at risk of cyberattacks and to show what possible actions can be taken to contain this danger.

Moreover, the safety of the society can be increased when municipalities are better prepared against cyberattacks and when the findings are applied in practice. As a result, sensitive data will not fall into the wrong hands.

Reading guide

The remainder of this thesis will focus on the theoretical background of the research topic, the methodology behind the current research, and the results, conclusion and discussion of the this thesis. The second chapter reviews previous literature about cyberattacks targeted at municipalities and ransomware attacks in practice. Chapter three will discuss the methodology that has been used during this research. It also contains a structure which was used as guidance for the interviews. The fourth chapter contains an analysis of the results that have emerged from the field research. Chapter five covers a discussion involving these results which lead to a conclusion in chapter six. Lastly recommendations are made for future research and limitations within the current research.

Literature review

This chapter will start by resenting a general theory on the origins of cybercrime followed by a literature review on the preventive measures of ransomware attacks. It concludes with a conceptual framework that will be applied to Dutch municipalities.

Routine Activity Theory

Routine Activity Theory (RAT) provides a holistic overview of criminal activity and helps in understanding how such activity can be evaluated. First formulated by Cohen and Fleson (1979) it has since been used in several applications to help explain criminal behaviour. This includes studies on domestic abuse (Leukfeldt & Yar, 2016), manslaughter (Akers, 2013), theft (Cohen and Felson, 1979) and vehicle larceny (Reynald, 2011). It has also been used by Chon (2014) to conceptualize the nature and implementation of criminal activity in cyberspace.

According to Cohen & Felson (1979), RAT helps analyse specific patterns of criminal activity at the macro and micro level through the evaluation of criminal trends. The structural model at the macro-level, covering the temporal and spatial patterns of everyday activities in society, is related to the situational model at the micro-level, which seeks to explain why a crime happens (Wikström, 2009). RAT can also be used to identify not just how criminal activities are perpetrated, but also to identify remedial mechanisms (Kitteringham & Fennelly, 2020, p.1). These findings imply that RAT can provide a framework to evaluate the reasons why a particular type of criminal activity such as ransomware attacks (RA) occur and how to prevent such activities as well.

According to RAT, for a crime to occur, there must be three elements. There must be a motivated offender, an appropriate target and the lack of a competent guardian (Leukfeldt & Yar, 2016). Motivated offenders are those who are not only able to commit criminal acts, but are also motivated to do so. A motivated offender is defined as any sort of individual who has a strong motive to commit crime (Glasser, 2015). The motivated criminal, however, must be someone who is also capable of committing the crime. That means that, the motivated criminal must have the mental and physical resources to commit the crime. A suitable target is any sort of person or property that the motivated criminal may easily disrupt or harm. The easier it is to target an entity, the greater the likelihood that a crime will get perpetrated (Glasser, 2015). A competent guardian refers to a person or an item that is successful in discouraging crime from occurring. The crime can often be halted just by the existence of guardianship in space and time (Leukfeldt & Yar, 2016). These views suggest that RAT evaluates criminal activity from not just the perspective of an offender, but relates it to the environment and its ecological processes.

The implication of RAT for this research is that ransomware attacks must be evaluated by (i) identifying the nature of the ransomware attack (offender and target); (ii) evaluating the processes and methods by which such attacks might be prevented (competent guardianship).

Ransomware Attacks on Dutch Municipalities

This section evaluates the nature of ransomware attacks on Dutch municipalities and conforms to the 'offender/target' element of RAT.

Ransomware has been defined as a form of malware that overthrows cyber-security mechanisms such as cryptography in order to access and hijack user data. Ransomware has also been defined in terms of a malicious software which infects computer systems through encryption and thereafter, restricting user access to files and data on the computer till a 'ransom' is paid (Atos, 2021, p.4). Some of the most common forms of ransomware include (i) crypt-encryption of files and data on computer systems in such a way that content is rendered inaccessible, (ii) locker attack which ensures that users are completely locked out of their systems, enhancing the urgency with which the ransom is to be paid within timelines specified by the cybercriminal; (iii) scareware which is the use of fake software that creates an illusion that a virus has been detected on the system and then to asks for payments to cancel out the virus; (iv) leakware where threat is made that sensitive personal or company information will be disseminated if payment is not made and (v) RaaS (Ransomware as a Service) ,where all actions are handled by the hacker, including distribution, collection of payment and recovery of the system (Kharraz et al., 2015, p.20). In summary, the underlying principle for all ransomware attacks is the recognition by cybercriminals of the importance of data, files, computer networks, digital resources to individuals, businesses and to hold these assets to ransom using various malicious methods, until a fee is paid.

Across the world there has been an increase in the number of ransomware attacks. According to studies by Kerner (2021, p.1), in 2021, the number of ransomware attacks doubled in frequency over that of 2020 and accounted for 10% of all cybercrimes. About 37% of global organizations fell prey to some form of ransomware attack in 2021 (Kerner, 2021, p.1).

There is growing instance of municipalities being targeted by ransomware attacks. These include the ransomware attacks on the municipality of Atlanta in 2018 (Chen et al., 2019, p.201), on the municipality of Durham of the state New Hampshire in 2016 (Maiorca et al., 2017, p.1720) and that of Baltimore in 2018 (Tuttle & Jacobson, 2019, p.33) all of which included requests for significant sums of money from the perpetrators.

In the Netherlands as well, there have been a spate of such attacks in the last 3 years, particularly in municipalities located in east Netherlands which have populations of between 30,000 to 50,000 inhabitants (Heppenhuis, 2021). A research of these ransomware attacks is necessary to identify their nature and what preventive protocols are currently being taken by Dutch municipalities.

In 2018, the municipality of Lochem was targeted by cybercriminals for several months, gradually hijacking several units of data before the attack was detected (Kuiper, 2020, p.1). The intent of the attack was to completely assume control of all computers in the system such that the municipality would no longer be able to access data, thereby jeopardizing government operations and tarnishing the

image of the municipality. By the time the attack was discovered and repelled by the municipality IT team, the cybercriminal had hacked deep into information and communication systems, installing hostage software, accessing sensitive information and inflicting financial damages of more than 200,000 Euros (Kuiper, 2020, p.1). It is still not clear how this attack was perpetrated, though it has been reported that the cybercriminals were able to leverage the open Remote Desktop Protocol (RDP) to access the computer systems (Kuiper, 2020, p.1).

In 2020, the computer systems of the municipality of Hof van Twente were targeted by hackers who were successfully able to 'lock' down the entire system (Smaal, 2021, p.1). During this period, the criminals were able to erase, encrypt and steal data , causing damage to the system estimated at over €4 million. A sum of €750,000 was demanded by the hackers but it was eventually not paid. This sum was demanded in bitcoins for the purposes of making it difficult to trace such financial transactions.

An analysis of the attack revealed that by using a relatively simple password "Welkom 2020", the hackers were able to access and stall the system (Smaal, 2021, p.1). Furthermore, the hack was facilitated by a change in the firewall settings. It became impossible to connect to the FTP-server used by the municipality to exchange files. Like in the case of Lochem, the hackers leveraged vulnerabilities in the Remote Desktop Protocol to penetrate the network. The most important finding was that penetration 'pen' tests conducted by the IT team at Hof van Twente municipality, were not able to detect the attack early on, giving the hackers opportunity to penetrate deeply into the systems (Smaal, 2021, p.1).

Similarly, in the ransomware attack in the municipality of Zutphen in 2020, the hackers exploited vulnerabilities in the Citrix servers to enter the system (Rufallo 2021, 1). The attackers were able to completely take over the system. However, the municipality was able to detect and repel the attack in time, before any damage could be done. Subsequently, an updated Citrix server was installed with superior ransomware detection and prevention capabilities.

Some of the key trends emerging from the research above are that ransomware attacks on Dutch municipalities invariably take the form of locker attacks as such attacks provide municipalities with limited options but to comply with the demands of the hackers. Firstly, these attacks are enabled by the increasing reliance of municipalities on computer systems and the internet. Secondly, these attacks are enabled by technological vulnerabilities, fewer resources and lack of knowledge on how to defend against such attacks.

Dutch municipalities, however, still do not know how to appropriately detect and prevent such attacks. There are few measures that unequivocally inform Dutch municipalities on how hackers were able to successfully penetrate sensitive data systems without being detected and repelled in time. In the next paragraph these measures will be explained.

Ransomware Prevention process

Studies on the prevention of ransomware attacks are not so much about the installation of preventive software on computer systems, but rather on the process as a whole. Literature indicates three distinct steps in any ransomware attack prevention process including (i) identification, (ii) prevention and (iii) response/recovery (Zimba & Mulenga, 2018, p.62; Grant & Parkinson, 2018, p. 322; Hull & Arief, 2019, p.22; Morgan, 2019, p.1). Accordingly, this section will evaluate literature related to each of these steps which conforms to the 'competent guardianship' element of RAT discussed in section 2.1.

Identification

Various approaches have been deployed to identify the presence of a ransomware attack. One of the most commonly used is the signature-based approach which detects unique 'signatures or patterns and sequence of bytes or the order of call functions and typical information in ransom demands etc (Grant & Parkinson, 2018, p.323). These signatures are incorporated into anti-malware software and enable the software to detect such patterns whenever a ransomware attack occurs. Goyal, Kakkar, Vinod et al. (2020, p.342) point out, however, that this approach is ineffective in detecting obfuscated codes, typically contained in ransomware and are hence unable to detect new forms of ransomware attacks.

Another method of detecting ransomware attack is the behaviour-based approach, which requires the observation of how malware operates with computer systems in a simulated environment including file access, system activity and network activity (Zimba & Chishimba, 2019, p.19). Grant and Parkinson (2018, p.322) investigated how ransomware behaves with underlying file systems in online networks and found that; each instance of ransomware displayed unique behavioural characteristics related to file system activity that were very different from those of normal user interactions. By identifying these patterns related to file access and user activity, it was possible to detect ransomware attacks.

Zimba and Chishimba (2019, p.20) applied reverse engineering on WannaCry ransomware and conducted source code analysis to discover the techniques used by ransomware to detect vulnerable nodes in a network. A similar research was performed by Almashhadani, Kaiiali, Sezer et al., (p.2019) on the Locky ransomware family, to identify how such ransomware tried to get in touch with CnC servers before delivering malicious payloads. However, the deficiency of current network behaviour approaches is that they still leave computer systems vulnerable to 'zero-day' attacks that can lock them down (Alshaik, Ramadan & Hefny, 2020, p.2).

Prevention

According to Surati and Prajapati (2017, p.4), proactive prevention is the best defence mechanisms against ransomware attacks. This requires organizations to recognize the reality of ransomware attacks and to take protective precautionary measures.

One of these measures is to educate personnel and employees on how ransomware attacks are conducted (Zavarsky & Kindskog , 2016, p.468). Al-rimy, Maarof and Shaid (2018, p.153) stated that ransomware attackers routinely use organizational endpoints, particularly non–IT employees, to access computer networks. This point was corroborated by Adamov and Carlsson (2017, p.6) who observed that because the target of ransomware attackers are mostly the employees of an organization, there is need of awareness and training programs on how ransomware attacks are conducted. For example, employees need to be told not to click on links sent through email that they find suspicious or irrelevant to their work or organization. In connection to this, Song, Kim & Lee (2020) recommended the use of simulation exercises to train employees how to recognize phishing emails through which ransomware attacks can be potentially conducted.

By installing secure electronic gateways for email and the internet, organizations can prevent ransomware attacks occurring through email (Saurbaugh & Liska, 2017, p.1). This view was corroborated by Goyal, Kakker and Vinod (2020, p.242) who recommended the use of strong spam filters that block malicious IP addresses, and prevent phishing emails from passing through organizational systems. Furthermore, they recommended the use of email authentication technologies such as the Sender Policy Framework (SPF), Domain Message Authenticating Reporting & Conformance (DMARC) and Domain Keys Identified Mail (DKIM) to detect emails that are spoofed. In this connection, Wolf (2018) stated the need for scanning all inbound and outbound emails to detect those that are suspicious and eliminate them.

Other recommendations are related to firewalls and include the use of patch operating systems and centralized patch management systems (Akbanov, Vassilakis & Logothetis, 2019, p. 22). It is also recommended to install anti-virus and anti-malware software in order to regularly scan computer networks and systems for suspicious emails (Shaukat & Ribeiro 2018, 361). Yet another preventive mechanism is to patch vulnerabilities that are identified as being high priority (Pool & Custers, 2017). This helps plug any loopholes in computer network systems that can be potentially exploited by ransomware attackers.

Studies by Hull and Arief (2019, p.19) established the effectiveness of deploying the principle of least privilege, with respect to privileged accounts. This involves providing administrative access for administrator accounts to employees only when absolutely necessary. Ami, Elovici and Hendler (2018, p.1614) interpreted the principle of least privilege in terms of ‘access control’ and proposed the need for an authentication process that would provide only authorized users with access to sensitive computer systems.

Winter, Ruiz and Army (2018, p.22) explained that after ransomware infects a system endpoint, it sends out a DNS query to a command and control (CnC) server for the purposes of exchanging encryption keys. Monitoring such queries to identify and resolve them can prevent ransomware from locking files through encryption.

The above findings indicate that prevention measures can be summarized as (i) education of workforce, (ii) firewall installation, (iii) regular patching, (iv) restricted administrative access, (v) system scanning and (vi) DNS query monitoring. Despite all these prevention mechanisms being useful, this thesis needs to determine which of these mechanisms are relevant in the context of ransomware attacks conducted on Dutch municipalities.

Response & Recovery

Should the above-mentioned preventive measures fail, it is important for organizations to have the capability to respond and recover from ransomware attacks. This section discusses some of the response and recovery measures discussed by various researchers.

Kok, Abdullah and Jhanjhi (2019, p.141) recommend the immediate isolation and removal of infected computers systems from networks to prevent the ransomware from attacking other units in the network. This includes isolation and powering off all affected systems that have not yet been completely infected by the ransomware. This can provide opportunities for cleaning and recovering data, containing the damage and preventing worsening conditions (Zimba & Mulenga, 2018, p.59). Other recommendations in this regard are to collect and secure all parts of the ransomed information that might still be uncorrupted, and to change all online and network passwords after disconnecting the system from the network (Caporusso, Chea & Abukhaled, 2018, p.72).

According to Morgan (2019, p.1) the best way to recover from ransomware attacks is to ensure a secure back-up that will enable the restoration of business and critical data. This was reiterated by Hull and Arief (2019, p.20) who stated that it is necessary for organizations to conduct regular data back-ups for the purposes of ensuring business continuity, irrespective of the threat of ransomware attacks. Furthermore, it is important to secure the backups as well. This is because some ransomware have the capability of locking up even the backups through a process called persistent synchronization (Grant & Parkinson, 2018, p.319). Therefore, backups must not always be connected to computers network systems that they are backing up.

Ransomware attacks are always conducted with the motive of collecting ‘ransom’ in the form of payments made by the victim organization to the hackers (Partida, 2021). Pool and Custers (2017, p.126) point out that after a ransomware attack has been effective in locking systems, all stakeholders including shareholders, employees and customers must be consulted on whether to pay the ransom or not. Some of the considerations here include the technical feasibility of recovering and restoring compromised data, time to do so and the cost of restoring and restarting systems from the backup (Pool & Custers, 2017, p. 127).

Al-rimy et al., (2018, p.150) however, do not recommend payment of ransom to hackers as such payments do not guarantee that the organization will be able to re-access their data. This point was corroborated by the US Department of Homeland Security (2020, p.4) who observed that some

individuals and organizations were not provided with decryption keys even after paying the ransom. Some organizations were targeted again by ransomware attackers after paying ransom (Grant & Parkinson, 2018, p.320). Furthermore, research by Wecksten, Frick and Sjostrom et al., (2016, p.1354) found that even after paying the ransom originally demanded, some organizations were told to pay more if the decryption key was to be provided to them.

These views imply that the underlying principle for refusing demands for ransom is that such payments can further encourage this type of cybercrime business model.

Law enforcement

It is imperative that law enforcement agencies are contacted to report ransomware attacks and request for assistance in detecting the source of such attack (US Department of Homeland Security, 2020, p.5). In the Netherlands, it is the National Cyber Security Centre (NCSC) that has the responsibility of ensuring that the country is resistant to internet crime (Nationaal Cyber Security Centrum, 2021). The NCSC in turn reports to the National Coordinator for Counter-terrorism and Security (NCTV), which indicates that in the Netherlands, cybercrime is associated with terrorism and breach of security (Ministerie van Justitie en Veiligheid, 2021).

The NSCS conducts a number of tasks related to digital security in the Netherlands including continuous monitoring of suspect sources on the internet and alerting authorities and organizations about viruses and website activities perceived as threats; providing advice to organizations on how to protect themselves from online threats and continuous monitoring of developments in digital technologies related to security systems (Ministerie van Justitie en Veiligheid, 2021). Dutch organizations such as municipalities must report ransomware attacks to the NSCS as part of responsible disclosure activity.

Article 138 (a) of the Dutch Civil Code (DCC) explicitly treats cybercrime attacks such as hacking and ransomware as a crime. This is evident in its criminalizing of individuals that intentionally and unlawfully access computer networks by breaking into security devices, through technical interventions and/or with the use of false signals or false keys (Overheid 1999, 1).

On December 2015, the Dutch government introduced the Computer Crime Act III (Wet Computercriminaliteit III) with the purpose of attempting to improve cybercrime criminal prosecution. According to Pool and Custers (2017, p.127) this new act proposes that investigative capabilities for authorities and law enforcement agencies are expanded. This includes criminalizing activities such as hacking into systems and installing spyware as well as those related to restricting or deleting files (Pool & Custers 2017, p.127).

Furthermore, the new act provides more powers to public authorities to counter cybercrime. Police and prosecutors will have the authorization to arrest persons that are suspected in trafficking in stolen digital information; to investigate or hack into the computers of suspects remotely including the

installation of software to detect malicious forms of cybercrime and intercepting offensive and harmful data to make it inaccessible to the general public (Ministerie van Justitie en Veiligheid, 2021).

The objective of these new powers is to enhance police capability to fight cybercrime effectively and to swiftly identify and punish offenders. Furthermore, the Computer Crime Act III may improve the investigation capabilities of the authorities as it allows them to engage with computer systems of citizens and enables them to make changes, copies and even delete data such as malware. However, this specific rule has been controversial as it is considered to violate the privacy of citizens (Van der Sloot, 2017, p.201).

Furthermore, the efficacy of the Computer Crime Act III has been challenged. For example, Oerlemans (2017, p.356) pointed out that the identification and localisation of a suspect can be very challenging due to the utilization of different methods related to anonymisation and Wi-Fi networks. Therefore, gathering sufficient evidence and linking it to the suspect becomes cumbersome. Oerlemans (2017, p.356) also sated that the increase in standard encryption lessens the effectiveness of detection methods already being used.

Additionally, Oerlemans (2017, p.356) also observed that jurisdiction has become a huge challenge due to cybercriminals being able to commit cybercrimes within the Netherlands while being located elsewhere. This point was reiterated by Pool and Custers (2017, p.127) who said that even though cybercrime can be an issue of jurisdiction, the efficacy of current law can be countered as its applicability is often determined by the state in which the offender computer system or device is situated.

The above views indicate that current jurisdictional procedures in the Netherlands offer remedy to victims after a cybercrime has been committed. However, even in the Netherlands, the efficacy of Dutch jurisdiction to detect and prosecute cybercriminals is limited. This means that preventing cybercrime activities can be more important than response and recovery mechanisms.

Conceptual Framework

Based on the findings in sections 2.1 to 2.3, the conceptual framework in figure 2.1 was developed.

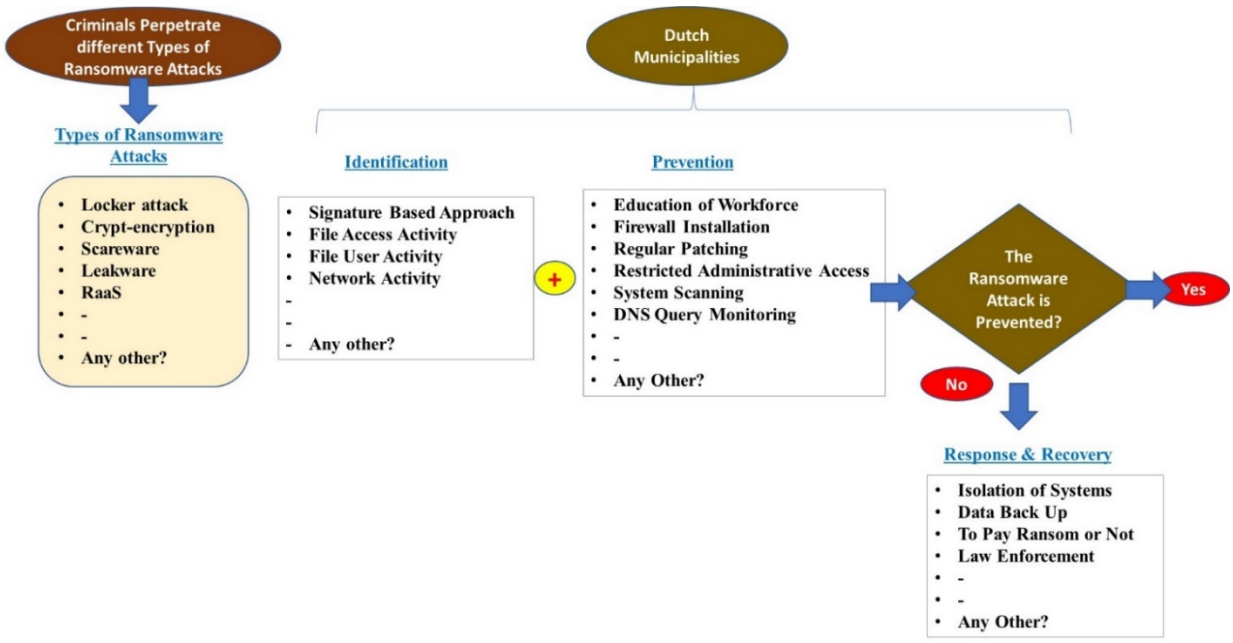


Figure 2.1. Conceptual Framework

From figure 2.1, it is observed that there are two entities involved in a ransomware attack. One of them is the criminals that perpetrate various ransomware attacks and the other is their victims, i.e. the Dutch municipalities. There are several types of ransomwares. However, this research will identify which of these are the most commonly occurring ones with respect to Dutch municipalities. It is possible that there are some types of ransomware attacks not discussed in the literature, but which are threatening Dutch municipalities.

Countering ransomware is a three-step process including identification, prevention, response and recovery as indicated in figure 2.1. In the first step, the municipality has to identify several different methods used by criminals to target their online systems. The second step, the municipality must be able to use different preventive measures to counter the identified ransomware attack. In the event that these preventive measures are inadequate to counter the attack, and the attack takes place, the municipality must implement a set of response and recovery measures that reduce the impact of the attack as much as possible. This is the third step.

There are various measures discussed in the literature with respect to each of these steps that are summarized in figure 2.1. This paper will identify which of these are currently being used in Dutch municipalities, how effective they are and what are the most effective ransomware countering measures given the particular types of ransomware attack that are currently threatening computer system in Dutch municipalities.

Methodology

Research methods

This chapter defines the approach to the main question and deals with the method in relation to the field research. The aim of the current research is to try and research different factors that may impact public organizations' capability of preventing cybercriminal activity, and remain proactive in safeguarding their data. The focus within this research is shifted towards the prevention of cybercrime within the public sector namely between two organizations, where one is doing noticeably better than the other, or between a public organization and a company with a good reputation regarding cybersecurity. Existing literature will be used for this comparison.

This research uses a qualitative method, namely interviews. Current and former employees who worked within this branch and are known as experts were approached and interviewed. Additionally, specialists on cybersecurity were also approached for an interview due to their specific knowledge on the subject.

Existing literature was used to determined which municipalities had experienced an attack. The literature was subsequently used to categories the municipalities as having undergone (i) a successful attack, (ii) an unsuccessful attack, or (iii) had never experienced an attack before.

Moreover, four municipalities were selected based on their geographical location. Of these four municipalities, two came from the East side of the Netherlands and two came from the West side. The difference in size of inhabitants belonging to each municipality was included in the selection procedure. To fall under the scope of this research, the municipalities where an attack has occurred within the last 3 years were considered to be relevant to this research. The municipalities whereby there have yet to be any successful ransomware attack had to meet the same requirements. This will help in conducting a complete investigation. IT experts were also interviewed in this research to gain better understanding of computer systems and possible gaps that cyber criminals.

The input of IT experts allowed the researcher to validate the claims from the interviews with the respondents from the municipalities. With the help of an example, the interviews were designed, and the respondent were able to offer input on certain issues that require specialist knowledge. The plan therefore was not to focus on what the organization or company is doing wrong but what the current state is like, and which components could be done better, based on possible risk from recent events. The aim was to interview employees from municipalities who fall under the scope of this research. The interviewees were selected based on experience and expertise. Data from interviewees and their municipalities were handled with confidentiality and were not traceable.

Data collection

This research has attempted to produce internal assessments of the scope of impacts. The impact of cybercrime attacks was assessed within the municipalities. The unit of analysis within this research is cybercrime prevention and the source of information is respondents who have insight into the possible attacks. The latter ensures the optimisation of respondents, as they are best suited for contributing to this research. It is important that there is the necessary knowledge and work experience regarding the current set-up of cybercrime prevention. From here, qualitative input was provided so that relevant statements could have been made.

Respondents

In order to be a suitable candidate for this research, the respondent had to meet certain criteria:

- The respondent should have knowledge on cybercrime in order to be able to provide relevant input.
- The respondent must be employed by the municipality, have experience working with the municipality's IT-department or have a Cybersecurity related role in general as it will give them a better idea of the possible impact.
- The respondents work for various municipalities, so that the issue can be viewed from multiple perspectives.
- The respondents should have at least one year of experience within the organisation.

These above criteria were used in order to increase the quality of the data because a distinction ensures that only a few respondents suitable for this research are selected.

In addition to interviewing respondents who fit the criteria states above, IT-experts within the industry were interviewed. They might approach the issue within this research from a different angle, providing interesting insights for recommendations and future research. In addition to the criteria stated above, the IT experts had to meet the following criteria:

- The IT-experts should have experienced a cyberattack.
- The IT expert has worked in companies with at least 500 employees.

With the help of key informants, the most suitable respondents were selected. Key informants are contact persons within an organisation who bring the researcher into contact with potentially suitable respondents. By means of the qualitative character of the research, room was given to the respondent to fill in the questionnaire as they see fit. Because a case study was used here, the examples given by the respondent could be described in detail. It is important, however, that the respondent is able to name a clear practical example in order to avoid subjective input.

Since the respondents in this research met the criteria, all their data were included. A total of 12 respondents participated in this survey. Seven of these are employed by a municipality, four are IT experts and one is employed by ROC Mondriaan as CEO, with extensive experience in this field. The table below shows where the respondents are employed, in which position and how many years of experience they bring with them.

Position	**Organization**	**Experience within organization**
Head of the department ‘’Leefomgeving’’	Hof van Twente	6 years
Head of the IT department	Zutphen	6 years
Policy Officer IT	Hof van Twente	11 years
Project Assistant	Leiden	2 years
Information Security Consultant	Zoetermeer	16 years
Senior Policy Advisor IT	Zoetermeer	5,5 years
Cybersecurity Consultant	Capgemini	3 years
Penetration Tester	Anonymous	5 years
CEO	ROC Mondriaan	1 year
IT-expert consultant	Aeon	35 years
Chief Information Security Officer	Leiden	2 years
CEO	SRS Secure Solutions	32 years

Table 1: Respondents

Interviews

The interviews took place in November and December 2021. Although it was the intention to do face-to-face interviews, due to COVID-19 measures, all interviews have taken place online. Nevertheless, this did not affect the quality of this research because the interviews were recorded and could be accessed at any time. This was tested through a test interview.

A test interview showed that the initial interview questions did not lead to a clear answer. For example the question ‘’How is cybercrime prevention currently organised in your municipality (infrastructure)?’’ was complemented by ‘’Which system is used?’’ Therefore, some questions were added that could be used to remove ambiguities, such as "Can you indicate what you mean by that?" or "Do I understand correctly that you mean the following?".

These adjustments were tested again in a test interview in which another respondent was questioned. It resulted in the interview being conducted more easily and clearer responses.

In order to avoid differences in terminology, these interviews have been conducted in English. This way, no ambiguities arise and no data were lost in translation by having multiple languages.

The same structure and order of the interview was kept, so that all respondents would be faced with a similar situation. For the researcher, however, it was important to be alert, because respondents sometimes answered follow-up questions without these having been asked already. As intended, the

moment of consultation was also used to make any changes to the answers given. In the end, one respondent (Policy officer IT) made use of this possibility and tried to answer the questions better with a few additions.

Interview format

Within this section the process of the interviews is explained, and detailed information is given on the steps for each phase.

Prior knowledge

Prior to the research, the interview candidate was provided with a clear understanding of the context of the research along with a definition of cybercrime (Appendix VI). This also promoted credibility by providing relevant information to participants before the interview took place (Saunders et al., 2016). This information was shared with the respondent no later than 3 days prior to the interview so that they would have ample time to gain knowledge related to the research which would facilitate the interview process. Prior to the actual interview, the respondents knowledge on the provided information was checked upon again by means of a control question to see if there are any uncertainties.

Interview steps

The respondent was welcomed, and the purpose of the research was indicated. During the interview the respondent was asked if recording is allowed so that the researcher can use it for further processing. It was explained that recording was necessary in order to process the data carefully. This way, the respondent was aware of the reason for this (Healey & Rawlinson, 1994).

In addition, ethical aspects were highlighted, stating that participation was on a voluntary basis and that confidential data would be handled with care and anonymity guaranteed. This was expected to enhance reliability and reassure the respondent in giving the most honest answers possible (Kılınç & Fırat, 2017). Afterwards, the respondent was thanked for their time and informed that a text version would be sent to them. Should there be any comments or additions, the respondent was given the opportunity to process this.

Substantiation of questions

It is important that the interview questions are understood by the respondents. In addition, it is also important that the researcher understands what the respondent means by the answer given (Foddy & Foddy, 1994). The interview questions are outlined below and a rationale for why they are asked is provided.

1) Introduction
    a) Are there any ambiguities about what is meant by cybercrime prevention in this research?

This question was asked in order to ensure the quality of the interview and so that it is clear in what context this research is taking place and what the framework is.

b) How would you describe cybercrime and are you familiar with the definition of ransomware?

For the quality of the answers it is important that the respondent has knowledge of the criteria. This question is used to check whether the respondent has fully understood the information form. Asking this question can remove possible ambiguities and is used as double check.

2) Additional questions

a) What is your role within the municipality?

Although a targeted search was made for respondents who work within the IT field, it is important to make it clear that this is actually the case. In addition, a healthy distribution of respondents is necessary, as this gives the opportunity to look at the issue from different angles.

b) How long have you been active within the municipality?

Because ransomware attacks are always lying in wait, it is interesting to know how long a respondent has been employed by the municipality. Based on the number of attacks and work experience, interesting patterns could be found.

3) Substantive questions

a) Have you ever experienced a cyber-attack within your municipality?

i) Yes (1): how did the municipality act here?

ii) Yes (1): to what extent has the municipality suffered a loss?

iii) Yes (>1): have you also seen possible patterns in different attacks?

iv) No: If you have not, can you imagine what risks there might be for the municipality?

This question is not only related to the previous question, but is also a stepping stone for the following questions. A respondent who has experienced an attack would be able to describe this experience with the help of practical examples.

b) How is cybercrime prevention currently organised in your municipality (infrastructure)?

i) Which system is used?

This question was also asked in advance (Information form, Appendix II). Understanding this can reveal possible connections and discover a cause-and-effect relationship.

c) How is cybercrime prevention currently organised in your municipality with regards to budget and policy?

i) Do you have insight into the costs associated with cybercrime prevention and weighs this up to the possible benefits? **(Specified with example)**

This question can provide insight into whether there is a link between the available budget and the vulnerability of a municipality.

d) Are cybercrime prevention methods and information being shared among municipalities to your knowledge?

On the basis of this, it can be determined to what extent there are collaborations between municipalities in the area of cybercrime prevention. If this is the case, it can also be investigated to what extent this has contributed so far.

e) Has your municipality adopted an infrastructure or strategy with regards to cybercrime prevention which is also being implemented at foreign municipalities?

This can be used to find out to what extent there are collaborations with foreign countries and whether there are certain shared strategies and infrastructures in this area.

f) What could be done to prevent possible attacks in the future?

i) Do you have any specific examples (e.g. at a previous municipality or employer)?

This allows the respondents to give their own input and insights on the subject. Respondents with previous work experience (both within and outside municipalities) can come up with angles to improve cybercrime prevention.

At the end of the interview, the respondent will be asked if there are any other matters that should be taken into account in the case of cybercrime. If the respondent indicates that this is the case, they will be given the opportunity to explain. This information could be valuable for the further course of this research and future research.

Within this research, the following conditions apply to increase reliability.

- The interview is conducted in a neutral environment, so that no room can be offered for possible influence (Saunders et al., 2016).
- The information form is provided in advance so that the respondent can familiarise themselves with the subject matter.

Data analysis

The recorded interviews were transcribed, after which respondents were given the opportunity to make any comments within one week. This period was kept short so that there was no unnecessary delay in regard to further data analysis.. When respondents did not react, another reminder would have been sent out. If there was no response to this reminder, the response would have been considered final.

After the trainscripts were coded, the results were subjected to analysis, from which conclusions will follow. This research is shaped by an inductive approach in which, among other things, specific observations are sought.

Coding

The transcripts were then coded to extract the most relevant fragments from the interview. Initially, the text fragments were analysed after which open coding took place. The first stroke involved open coding, where the arguments mentioned are dealt with. Next, axial coding was done to find out whether these are mentioned more often by different respondents. The coding process reveals important aspects indicated by the respondents with regard to cybercrime prevention. By linking these together, it is possible to weigh up the degree of importance and gain insight into how often certain aspects are mentioned. For example, there may be differences in how respondents name image damage. One respondent may talk about "image issues" and the other about "reliability damage". By linking these, a situation arises in which the underlying argumentation is filtered on different terms from respondents. These are rearranged in the research and come under the variable "image damage".

Reflection

This section elaborates on the reliability, validity, and ethical aspects within this research.

Reliability

In order to facilitate the reliability of this research, several choices have been made. Firstly, the steps within this research have been described in detail. Because this is the case and because it is clearly explained how and in what order the steps were carried out, other researchers should, in general, also come to the same conclusion if they had conducted this research with the respondents who were interviewed within this research (Gibbert & Ruigrok, 2010). The term 'in general' is used here because it is a subjective assessment by the researcher. To increase reliability, it is also substantiated why certain questions are asked and why they are included in the questionnaire. To ensure that reliability is positively affected within this research, the respondents were given the opportunity to rate their own input.

The use of semi-structured interviews means that there is a certain degree of flexibility, for example, to respond to topics by means of follow-up questions. Although this has its advantages, it also makes it difficult to repeat the same interview. This is because reality reflects the moment of the interview and therefore a change of situation is always lurking (Saunders et al., 2016). This research tries to overcome this by dealing with the technical design in such detail that it is possible to trace how data was collected and how it was analysed. However, it is important to note that organisations may be subject to changes at both organisational and human level in order to combat cybercrime.

Internal validity

The conclusions within this research are the result of desk research and qualitative research in the form of interviews. The framework for the interviews ensures that the execution takes place in the same manner each time (Verhoeven, 2014). In order to carry out the processing of these interviews accurately, the raw data was first coded before any conclusions could be drawn. Because the analysis of this is carried out by the researcher, and therefore individually, this can lead to bias.

In addition, the interviewer has adopted a neutral stance so that the tone and/or behaviour of the interviewer would not influence the respondent's results. Moreover, the interviews were also recorded with the respondents permission. This was done verbally. By recording the interview, the researcher had the opportunity to listen to fragments about which there was doubt. This allowed interpretation errors to be re-listened to several times, which increased the reliability of transcribing.

External validity

Within this research, 12 respondents were interviewed to find out how cybercrime prevention can be improved within municipalities. The research complies with analytical generalisation, because the data from interviews can be directly linked to theory. The possibility for improvement and experiences can also occur within other municipalities, which makes this research largely generalisable within the Netherlands. The extent to which this can be generalised on an international level is difficult to estimate, because within municipalities there may be other methods and other technologies in the area of cybercrime prevention.

Construct validity

By reinforcing the terminologies in advance, it measured what was intended. Triangulation was used within this research. Various sources have been used such as interviews and a literature review to determine the impact and consequences of cybercrime. Validation of the answers has also taken place after the interviews. The respondents in this study were able to inspect the completed interview in writing. If changes needed to be made, they had the opportunity to do so. This prevents the unjustified recording of data to be used in this research. A risk that lurks when using interviews is that socially desirable answers can be used. By processing the data anonymously, partly due to the AVG legislation, an attempt is made to reduce the risk of this happening.

It is important that the design of the questions and use of the instrument is of sufficient quality to allow for accurate observation of reality (Gibbert & Ruigrok, 2010). The questionnaire was therefore administered to a test subject. This test subject was comparable to the actual respondents and in this way, possible errors and ambiguities were eliminated and the questionnaire refined. This research also depended on the willingness of respondents. After all, they had the freedom to participate, but they also had the freedom to fill in the details about a certain subject. If this did not happen to an sufficient extent,

there would have been a risk that the data obtained will not have been an accurate reflection of reality. To overcome this, the interviews were recorded. This was done with the consent of the respondent in order to prevent possible incompleteness. Should the situation have occured that respondents did not want to be recorded, they would have been replaced by the respondents who do agree to be recorded.

Ethical aspects

Because ransomware attacks on municipal governments is a sensitive subject for the governments and those who work within them, it is important to process the research results on a morally sound basis (Saunders et al., 2016). In order to guarantee the quality of the data obtained from field research, the following points have been drawn up.

- A confidentiality agreement will be signed beforehand
- Participation in this research is voluntary. In addition, the respondent has the opportunity to withdraw at any time.
- The input of the respondents cannot be traced back to the respondent or organisation
- After completion of the interview, the respondents are given the opportunity to view the transcribed interviews. On this basis, they can agree with the content or make changes.

Because the recordings were made, the equipment is made available to the respondents. For sensitive subjects, the respondents were able to indicate whether they were prepared to answer questions without this being recorded. Should this be the case, a note will be made so that this can be presented for validation (Saunders et al., 2016).

Analysis

This chapter contains results that emerged from these interviews. From the results, the following aspects emerged as most important. This did not only involve looking at how often an aspect was mentioned, but also at the underlying reasons why this was the case.

Two-factor authentication

The results of the qualitative research show that two-factor authentication is a frequently used method to promote the protection of organizations. The importance of this is underlined in the case of Hof van Twente. By means of a brute force attack which is a hacking method that uses trial and error in order to crack passwords, the hackers tried to get into the system via 100,000 automatic attempts with the use of a programme that cracked the password. They succeeded within three weeks. If the password would have been more difficult it would have taken half a year, but they would still have got in. However, if there would have been a two-factor security the hackers would not have gotten in through a brute force attack (respondent 1). Hackers often acquire programs on the dark web that go through all the numbers and letters before the right password is found.

As said a two-factor authentication will prevent a brute force attack from getting through to the system. It is also possible to use workplace login details to log into applications. If this is not possible the Two-Factor authentication is the minimum requirement to have (Respondent 12). It is striking, however, that not all municipalities have been using this two-factor authentication method.

An example is the municipality Hof van Twente which had not implemented the method until after the attack had happened. Nevertheless, it emerges that two-factor authentication is not used throughout the municipality. It is in fact mentioned that a two-factor authentication application is sometimes used, but that this is not required for all activities (respondent 4).

To cut off the possibilities for attack, ROC Mondriaan has opted, for example, to make the two-factor authentication also compulsory for users of the system, including students. By being consistent in this respect, the intention is to counteract any weaknesses (Respondent 10).

According to the IT-expert (Respondent 11) many individuals just use Microsoft OneDrive or a Google-like system for accessing files. To reach these files, these individuals make use of the two-factor authentication. However, when sharing these files with others who do not have two-factor authentication, the effectiveness lessens greatly due to the user bypassing the security method but still having access to the files. It is impossible to state: 'I only want to admit people who have really good security'. The incidents are at times when the security was less strong though.

According to a Senior Policy Advisor IT (respondent 7) cybercrime prevention is not just typing a few codes into the terminal. A layered security is recommended, and this not only directed at a technical

layer but also on processes. If processes are not well structured, problems may occur which could be abused.

It does not necessarily have to be an external individual, sometimes it can also be an internal employee which are called insider threats. The best systems can be used, but if the staff is not aware of how they are to be used in a safe manner, the risk of a threat increases.

Two-factor authentication however is an aid but not a general solution for all cyberattacks, and in particular ransomware. It is only a piece of the puzzle but a major contribution to security. With a two-factor authentication it will be possible to check from which location certain login attempts are made. However, this is not unique to Two-Factor authentication.

Staff training

It is important to invest in awareness on an ongoing basis. It is seen that both municipalities and companies require that their staff must take a mandatory exam preceded by video workshops (Respondent 2). People who don't pass those exams are obliged to participate in a resit up until the moment they pass.

The municipality Hof van Twente makes sure that employees are aware of the importance of good passwords and Virtual Private Networks (VPNs). Additionally, the municipality also forbids the usage of public Wi-Fi networks for work purposes to reduce malware attacks (e.g., ransomware).

Although individuals are trained to know about cyberattacks, the hardest part is to get it to a manageable level for the users (Respondent 11). It is important to pay attention to it as an infrastructure manager and it is also necessary to train users to demand security from their parties with whom they share data with. In turn they should also sufficient protection. This is often underestimated by municipalities (Respondent 4).

Municipality Zuthpen teaches their staff to turn on the VPN when working from home or when on a different network is being used other than that of the municipality. This is emphasised within the e-learning programme during which skills are taught with the goal of raising awareness on the different aspects cyberattacks and its prevention. This includes visits to various departments, webinars, training sessions and roadshows.

According to a Cyber security consultant (Respondent 7), it is pivotal that this also happens within municipalities. It is important to teach the staff basic knowledge and to keep testing them by sending fake phishing mails or using fake breaches with the aim of keeping them cautious. Also, according to this Cybersecurity expert (Respondent 8), awareness is the most important factor because attacks can come from all angles. The respondent further emphasized that most of the attacks come via phishing attempts and end-user computers. That is why it is important to continue to help employees make the right choices. Roadshows are extremely useful due to their creative and playful nature. Otherwise, it quickly becomes enforced and that can lead to employees not reporting anything out of fear.

According to the cyber security expert (Respondent 8), it must also be made clear that 100% security cannot be guaranteed.

National organised system

Currently municipalities are missing the central overseeing point which commercial organizations possess. It is a lack of central policy which makes it that municipalities do not use the same software. Investing in SIEM and SOC is a solution which is increasing rapidly. However, there is some confusion over what the difference is between a SIEM and SOC.

SIEM

SIEM stands for ‘’Security Information and Event Management’’ and is basically a collection of tools which provide a constant and real-time view of an organisation’s IT infrastructure. This information is needed to aid security teams whereby threats are detected. The early detection enables one to effectively manage security incidents. Once a threat has been detected it immediately sends alerts to analysts which allows them to respond to risks quickly and effectively.

The SIEM approach is a combination of 2 earlier adopted methods: SIM and SEM. SIM stands for security information management and SEM stands for security event management. SIEM is a powerful solution, especially in evolving cyber threats and more specifically ransomware attacks. This does not mean that the system is completely protected however, since there are some limitations in play.

First of all, it is costly and time consuming. Using a SIEM solution requires 24 hours monitoring. In addition, a SIEM solution also needs maintenance and configuration where this also depends on the size of the organisation. To implement a SIEM solution a full-time team of experts is needed, which is also an economical expense to an organisation. The ability to manage a SIEM solution depends on the extent to which a municipality is able and willing to bear this. In line with this a few of the alerts could be false positives. Although they do not need immediate attention, an analysis in inevitable since there must be certainty that there are no legitimate ongoing attacks going on which should require attention from the IT department.

Another issue with this method is that although more information and logs are collected, it could lead to an overload of data and alerts which could result in a reverse effect on workflows and productivity (Respondent 5). Nevertheless, the advantages may outweigh the benefits.

SOC

If a municipality wants to make use of the SIEM method, it should also make use of a security operations centre (SOC) for the best possible result (Respondent 11). While SIEM is the set of tools used to identify, monitor, record, and analyse security events, a SOC complements this technology with the resource needed to manage it. This includes a team of dedicated security experts that use SIEM tools to continuously monitor an organisation’s IT infrastructure, search for threats and respond quickly to any

attacks. By adopting SOC, organisations and municipalities could provide themselves with an extra form of defence. Here it does not matter whether attacks are internal or external or even the type of attack which can also counter ransomware.

Using the SOC method also provides a quicker response time which could limit the amount of damage caused by a ransomware attack. This also includes reputational, financial and/or operational damage.

The municipality of Leiden has switched to a new workplace but there is still Citrix software in the underlying infrastructure. This in itself is not really a security measure, but more of a tool. Though the risk is always present, it is possible to prevent malicious parties from getting into the network. The municipality of Leiden therefore set up measures, such as a SOC service and a Security Operations Centre which monitors on the outside whether strange things are happening, where people are trying to break in or that certain systems are being broken into or log in attempts are being made to see if people or someone can get in (Respondent 12).

By detection, a SIEM SOC solution is meant that detects suspicious traffic flows from the Internet and on the internal network. Detection through the preventive measures taken, for example the actual detection of a virus and response, which stands for the ability to respond quickly to a report/incident by applying the Security Incident Process.

Setting up a SOC-service enables to reacts to possible attacks. It's just like a burglary in your house, if you have your window open and the doors open and your neighbour has everything locked and barricaded, then yes, they won't go into your neighbour's house, they'll go into yours (Respondent 12). This works the same way with a cyberattack because hackers scan the network all day long to see where there are systems with doors open that have vulnerabilities and yes, if they pass by an organisation and the systems are not vulnerable and they are up to date, then yes, they will go to the neighbour and if they do have a vulnerability, leading to hacking them eventually. So, SOC is one of them, so it monitors and can react if things go wrong, but it is much more important to make sure that you are not the candy shop for a hacker and that they come and look at you.

SIEM SOC

The head of the IT department of Zuthpen (respondent 2) sees a support base for a nationally organised system regarding SIEM SOC where most of the municipalities in the Netherlands are involved in. However, this concept has yet to be implemented.

The policy IT officer of municipality Hof van Twente (respondent 3) has spoken to colleagues from other municipalities during which they came to an agree that the security measures at the municipalities are mostly at minimum level. Therefore, it is widely believed that SIEM SOC is of the measures that should be in place nowadays. The interesting thing is that the VNG (Vereniging voor

Nederlandse Gemeentes) participated in a tender in which SIEM SOC was planned to be implemented. Due to lack of centralized policy and resources, it did not go through at that moment.

According to an Information security consultant (respondent 5) SIEM SOC is upcoming since several years. However, just implementing SIEM SOC is not a solution in itself. With this solution even more log sources could be linked and a configuration can be made when to be alerted, and when not. T

he most important part of discovering abnormal threats is to determine what deviates from the norm and what is different from normal. Typically, in order to work with SOC a SIEM is needed. SOC encompasses the SIEM technology whereby team of analysts and engineers are present. These identify, analyse and respond to cyber security threats, while continually working to prevent attacks. However, a cyber security consultant (respondent 7) claims that in company specialists in this area is just very scarce because the commercial organizations are also looking for these specialists. There is high chance of a difference in pay between a (commercial) company and a municipality. This could make commercial companies a more attractive employer in comparison to municipalities.

The CEO of ROC Mondriaan (Respondent 10) states that municipalities want too much of everything, especially when looking at local governments and the tax that is spent. Apart from that, from a security point of view working together and daring to make choices it enables to create a much safer system with much more security because everyone is working on the same principles.

There are a number of preconditions of implementing SIEM SOC. It has to be active enough for organisations, because that it where it often goes wrong. Certainly, a SOC can take a lot of the fuss out of having those specialists in a certain number of places. It is important to think very carefully about the organisation around it, what processes and agreements you make whereby it provides real added value. SIEM SOC is an efficient use of scarce knowledge and resources, but then you will have to implement it very well (Respondent 11).

The Chief Information Security officer of municipality Leiden (Respondent 12) mentions that it is critical to have a centrale systems which shares the responsibility with municipalities and the suppliers of software. It has to be a joint effort of several companies that agree with each other that you just have to work together on this. Municipalities should start to see this more as a utility. Then it becomes easier to explain that you can use the same thing together. Everyone has their own wishes, but all the processes are basically the same, so you would have to weigh up user convenience versus security and also make a business case for it (Respondent 11).

Zero trust computing

Zero trust computing is a strategic initiative which helps prevent data breaches. This is done by eliminating the concept of trust within the architecture of an organization’s network. According to an IT-policy officer (Respondent 3) this is the approach that needs to be chosen from the moment an infrastructure is built outside the environment of the organization. That means that endpoints on laptops

have certain software that detects strange behaviour. The moment that the service starts to show abnormal behaviour, starts to communicate with (foreign) sources or when a script tries to run unauthorized it will be blocked and signalled to the administrator. According to the Information Security Consultant (Respondent 5) it has been made mandatory for government institutions in the United States and it should be implemented in the Netherlands as well. Even though this method has been utilized for some time now, a mandatory status would be more effective.

Costs and benefits

Results within this research show that the measure on security depends on how much it costs. The costs are also taken into account when the system is encrypted, and staff is not able to work anymore due to disruption of the workflow (Respondent 2). At that moment, the costs and benefits are weighed against each other. It is, however, evident that a cyberattack does not necessarily result in image damage for an organization. The amount of image damage having been done depends on how much the media is aware of the attack and of how transparent the organization decides to be about it (Respondent 1).

According to the Senior Policy Advisor (respondent 6) budgets differs between (commercial) enterprises and municipalities. It occurs that within municipalities security and safety are not fully addressed up until a breach occurs. However, this point appears to vary from case to case since a Cybersecurity Consultant (respondent 7) emphasises that commercial organisations concentrate on turnover to make enough profit and they see security purely as a cost.

Municipalities should have a different mindset since they have a budget for security prevention. In practice however, not enough attention is paid to this. When an attack occurs, municipalities would like to be back online as soon as possible so that they can resume to serve citizens and entrepreneurs (Respondent 1 & 2).

Although the payment option is a possibility, the pros and cons should be weighed. The Prosecutor's Office, the IBD and the VNG (Association of Netherlands Municipalities) advise against payment. This is a very brave decision and principled stance, and it may also be a sign that municipalities do not allow themselves to be extorted, which makes them a less attractive target. Another point is that payment does not guarantee the removal of the ransomware. With discrete information however it becomes harder to consider rebuilding an entire environment within a few months.

The most important point is to assess the damage and if it worth repairing or rebuilding from ground up (Respondent 5). Municipalities have specialized teams in order to cope with these kinds of issues though, both within as well as outside the organization. According to Cybersecurity Consultant (Respondent 7) the choice of ransomware payment over that of a system recovery is chosen more often by organizations even though the tools to solve the issue are available. Even though the resources are available, a cost-benefit analysis has shown that paying can be more advantageous depending on the particular situation. But in case of a municipality, it is still difficult to negotiate with attackers.

Respondent 3 from municipality Hof van Twente recalled that they cannot morally afford to go into business with criminals, so it was a principled decision not to deal with the ransomware threat because of extortion.

According to the IT-experts (Respondent 11) not all municipalities have a choice to make a cost-benefit analysis. This is because not all of municipalities have a high enough budget to pay a ransom. So, the factors that play a part that consideration vary from 3 factors: ethical to economic to image. The Chief information Security Officer from municipality Leiden (Respondent 12) has insight into the costs involved in preventing cyber incidents. This is actually a sum of various factors and the technical and organisational measures taken. This certainly outweighs the benefits. For example, in the case of a ransomware attack, an organisation must deal with ransomware (which government bodies usually do not pay on principle) and high recovery costs, especially if the ransom is not paid, it may be necessary to rebuild systems completely.

Own policy

Each municipality has its own budget regarding ransomware prevention methods. Respondents 1& 2 claim that municipalities do not share methods or information with each other. Although there are similar guidelines, the municipality ultimately makes its own choices and therefore there is a lack of standardisation among them.

Municipalities in the Netherlands have various budgets depending on several criteria including size and number of citizens. The budgets are subsidised by the central government through municipal funds. The municipalities are free, within established frameworks, to spend these amounts as they see fit. This also applies to ransomware and cybersecurity in general since municipalities are not bound by any specific set of guidelines or policies.

The only prerequisite is that the requirements set by the Baseline Informatiebeveiliging Overheid (BIO) are met. This includes the use of security software, security supplier and the type of risk management. Municipalities usually use external systems which they purchase from several suppliers which includes commercial applications. Respondent 3 from the municipality of Zutphen even declares that municipalities mainly manage part of it themselves on their own servers. It has to do with the fact that in the Netherlands there is no fixed policy for municipalities regarding security software or systems (Respondent 11). This indicates that a governmental obligation, for example, is still lacking.

The Cybersecurity Consultant mentions that companies are increasingly obliged to arrange certain things and that you can also be fined for. This occurs if you cannot demonstrate that you have your security in order. Because nowadays, of course, there's still a lot at stake, and there are organisations that are part of the vital infrastructure. It is questionable why it does not apply to municipalities yet. It would be a proper starting point according to respondents from the municipalities (Respondent 2, 3 & 6).

Within municipalities it is important to maintain a good password policy and be able to explain that well to your users, combined with the right behaviour, how do you deal with data and therefore dare to take decisions as an organisation. Because of this, passwords should not contain names and/or numerical combination. The most important part however is that it should not be required to change passwords at regular intervals. Regular password changes are demonstrably, empirically bad security policies according to the IT-expert since they lead people to create weaker passwords, because of the increased cognitive load associated with having to constantly re-memorize them (Respondent 12). The respondent refers to the fact that this is well-known in security studies, if not well-practiced by bog-standard IT departments.

Image

Since it is important to protect citizens data, municipalities like to propagate the fact that as a local government organisation that they ought to be reliable and dependable. There is a lot of financial risk for organisations and according to respondent 4 in the Netherlands alone about several millions of Euros are involved. However, if a successful attack would occur it could have a negative effect on the image of the organization as well.

Image damage is very difficult to express in money, that is actually what they call risk management (Respondent 7). It is about how much risk you have and the possible consequences of such risks. Image damage can be reduced when being transparent to the public and media. However, most of the times when attacks occurred municipalities did not react until the information had already become public which is unfortunately the way a lot of organisations get the incentive to start looking seriously at security (Respondent 8).

Respondent 5 takes us through a situation whereby the Municipality of Zoetermeer made the news in the local part of the Algemeen Dagblad, whereby a failure card was addressed. It was an initiative that is now called ‘’Basisbeveiliging’’ where it was analysed how they deal with certain security standards. It is admirable how transparent they have been about this and could lead to being an example in various presentations in the coming years across municipalities. Although this may be of added value it does take courage to act this way as a municipality.

Furthermore, is evident that a cyberattack does not necessarily result in image damage for an organization. The amount of image damage having been done depends on how much the media is aware of the attack and of how much the organization decides to share about it. Respondent 1 from municipality Hof van Twente pointed out that the amount of image damage became considerably less due to the fact that their municipality was being transparent to the media and its citizens right from the start. Getting hacked is becoming more and more normal however (Respondent 10). According to him it is also about how the press deals with the attack. These situations require delicate action and the press can become a liability if they decide to make it public during the early stages or without the organizations consent.

Additional findings

Within this section, themes are addressed which, although not often mentioned, are important for the completeness of this research.

Lack of knowledge

Individuals did not understand sufficiently that what they were doing constituted a risk. In addition, the municipality Hof van Twente had nothing in place to detect possible intrusions or to be able to detect hacked systems.

If a phishing mail was sent to a municipality where the staff is untrained, it is far more likely that the email will be opened. In addition, e-mails have also become more and more common. In fact, all the attacks that have occurred via e-mail where users have clicked on links that they should not have clicked on (Respondent 11).

Some municipalities have a whole team of experts who have experience with this and understand how it works, but a lot of municipalities also have someone in a Chief Information Security Officer position who is available few days a week. Because it is then mandatory, someone is appointed or someone who used to do the bookkeeping is appointed as CISO yes that is not someone who understands cyber security on a holistic basis (Respondent 11).

Use of firewalls

The Head of the IT department (Respondent 2) mentions a situation where hackers logged on to Citrix and then there's a firewall behind it and they did not get through. Individuals seem to believe that by putting a single firewall in the network they have good protection (Respondent 9). By using antivirus software on endpoints, they feel that there is a certain level of good protection and leave it at until they find that they do get a cyberattack. Once that occurs new service firewalls needs to be purchased and that is a costly operation. An internal firewall means better protection on several levels although continuous investment is needed to keep security up to standard.

Increased budget

After the successful attack, the municipality increased its budget so they are now rebuilding their security from the ground up, which will make them the most secure municipality in the Netherlands (Respondent 1). Especially with hostage software, it takes down the whole organisation, and there are very professional organisations behind it that have much more time and budget to do this sort of thing. Additionally, the chance of being caught is very low which means budgets need to be increased, where possible, to cope with this.

The software security budget has been raised somewhat within ROC Mondriaan (Respondent 10). It is believed that municipalities should follow this example (Respondent 11). New software packages

should be acquired which allows the security to be raised again. According to the Cybersecurity Consultant (Respondent 7) this will grow a little in the organisation, so it's not as if the budgets for software are going to be raised very, very high at once, specifically for each package. So the budget will have to be used effectively.

Increased security measures

Doing everything yourself as a local authority means that you have your own separate ICT department which is responsible for creating and maintaining software for you 24/7, for keeping your systems up to date and for improving them. Each local authority would then have to have its own IT department. But if you also purchase everything, then the monthly costs will also increase tremendously (Respondent 7).

Ten years ago there was no cybersecurity expert team or penetration testers because there was nobody who believed that they would be needed. This shows that developments are taking place at a rapid pace.

Endpoint security is one of the developments that has taken place. For example when a file enters someone's computer with an unknown signature that file can be blocked. By rebuilding systems it is opted to strive for a higher level of security moreover, several things need to be considered such as investments in your suppliers, external parties and reinstalling software. A bit of network segmentation will never prevent cyberattacks, but it does prevent the big leaks. Investing in this makes it that right direction is chosen.

Respondent 12 from municipality Leiden mentions that there is a new workplace now because many people work from home. It was always impossible to work from home with a token or with a code on the mobile phone. In addition, administrators use this as standard for logging in, and SAAS applications are used more often which makes use of Single Sign On, which is linked to your workplace account and which remembers passwords, so it is not necessary to have to use separate passwords everywhere and that is already a kind of secure link. Sometimes it is not necessarily suppliers.

When noticing that Citrix is not watertight, it is an easy way out to exclude Citrix from use. But Citrix is not sitting still either, they know in no time where their weak points are and will close them solidly (Respondent 11). Then you could suffer an attack from another type or another brand. So whatever software you choose, you will always have to set up a system where you say there must be an overarching controller system that keeps an eye on the packages. In the end the software supplier takes the necessary measures to close the security gaps, so it is currently reactive, and that approach needs to become proactive. The problem, however, is that hackers do not sit still and therefore you cannot blame a software provider alone.

Information exchange

The municipality of Lochem would like to share the lessons they learned (Respondent 9). The conference which is on the yearly basis (Utrecht) is a combination of a trade exhibition and conference. Again, this is voluntary. If municipalities manage it together, the advantage is that they can exchange data with each other about numbers and about leaks that have been found. It does not even have be a municipality (Respondent 11).

There are now more and more developments whereby cyber security companies and authorities in the Netherlands, that are concerned with cyber security, are paying more attention to it centrally and are exchanging information with each other about it, within and outside the sector. In addition, the IBD supports with various security products such as handbooks an exemplary approach and supports when an organisation is hit by a cyber incident. Respondent 7 of the municipality of Zoetermeer indicates that they hardly use it in practice.

Information Security Service

Municipalities are affiliated with the Information Security Service an organisation that is based on the Association of Netherlands Municipalities (VNG). It is used to monitor traffic, but they also warn about critical patches (Respondent 2). Because of a number of other incidents, a kind of joint service was set up under the VNG (Respondent 3). The aim is to raise the level of knowledge development in the municipality, and they also try to stimulate the exchange of knowledge and skills between the municipalities themselves.

Municipalities work together on the basis of the BIO, which stands for baseline information security for the government, and we are supported in this by the information security service, which also acts as a sectoral CERT, or Computer Emergency Response Team (Respondent 6). Via this route information is (partly) shared from the attacked municipalities. Municipality Hof van Twente shared information for example via this route, however it is not the case that a solution is necessarily being worked on together. Additionally the level of knowledge of the individuals is also very different in all municipalities.

Findings and discussion

This section discusses the course of this research and presents the findings in relation to the sub-questions. This is used as a prelude to the conclusion.

Results

Because only a few municipalities were included in this research, the question remains whether all possible dangers and points of attention have been identified. By means of interviews with additional municipalities it is expected that the majority of these have been covered. The fact that the issue has been viewed from multiple perspectives creates intersubjectivity, which has a positive influence on the reliability. For the sake of completeness, all steps within this research have been written out, which will benefit the reproducibility of future research.

The researcher has chosen to question respondents who work in different positions. The idea behind this is that the issue is treated as comprehensively as possible and that multiple perspectives come to light. This contributes positively to the validation, because a possible assertion or idea can be confirmed by several parties.

Although conducting the interviews and coding was a new phenomenon for the researcher, a test interview helped to make sense of this. A disadvantage of interviews, however, is that they are snapshots, and therefore an attempt was made to overcome this. If it turned out that there was a lack of clarity in the answers during the interviews, a follow-up appointment or e-mail was set up in which the respondents were given the opportunity to provide clarification. All respondents indicated that the interviews could be recorded. A few indicated that the part with name, function and municipality should not be recorded. The recordings ensured that the processing and coding were speeded up.

In one case, there were 2 employees from a municipality who wanted to conduct an interview at the same time. Nevertheless, at the request of the researcher, individual interviews were chosen, as this would probably reveal more information. In addition, this would facilitate the processing of the interviews. In order to execute the coding as well as possible, the transcripts of the respondents have been copied verbatim and have been included in Appendix V. With the axial coding, an umbrella term has been used which has been determined at the researcher's own discretion. This does, however, allow for subjectivity. Another researcher might arrive at different coding when following the steps, but this should not affect the outcome of this research. The sub-questions that were formulated prior to the study will be addressed. They will be dealt with separately below.

''How is cybercrime prevention against ransomware currently configured within municipalities in the Netherlands?''

Municipalities in the Netherlands have different budgets depending on their size, the number of citizens which fall under them, the age of the citizens and the number of citizens receiving benefits. These budgets are subsidized by the central government through municipal funds. The municipalities are free in spending the budget as they see fit as long as they can justify the expenses to the government. This also means that municipalities are not bound by any specific set of guidelines or policies when establishing their own cybersecurity against cybercrime and more specifically ransomware as long as the requirements set by the Baseline Informatiebeveiliging Overheid (BIO) are met. This includes which security software or system they decide to use, which security supplier they decide to work with and also what sort of risk management they want to follow.

An example of this is the municipality of the Hof van Twente where a successful ransomware attack had occurred. The municipality had been using Citrix on their security systems but had not implemented a two-factor authentication within their cybersecurity protocols which had ultimately contributed to the success of the ransomware attack. As respondent 3 pointed out ‘’If we would have had it, then it would have been virtually impossible for that to happen’’.

Additionally, the municipality of Zutphen experienced a similar ransomware attack while using Citrix on their systems, the attack however had not been successful at this municipality. According to respondent 2 ‘’The chain is as strong as the weakest link, and they had or have RDP things that we did not have for years and that two-factor authentication you cannot get out of it with us, it is everywhere’’. This implies that if a municipality has a 2nd layer of defence after the implemented software which is this specific case Citrix the chances of a successful ransomware attack can be considered lessened.

The Municipality of Leiden has been using Citrix up from 2003 to 2020 after which they decided to switch their systems to that of Legio. In accordance with Legio the municipality also uses VPN ware along with 2 factor authentication.

The municipality of Zoetermeer does not use Citrix but a VM-ware, the user uses a local and a virtual workstation. The virtual workstation destroys itself when the user logs out of a remote or local workstation. With regards to security measures, users are not free in installing software. Additionally, the municipality’s security software is located in the Microsoft 365 section, and therefore in the Cloud section and on the workstation. Thus it is a combined system not a separate one, both systems communicate with each other so the user does not have to look for problems within them separately. Furthermore, the network is divided into compartments. This mean that if a user decides to go onto their server environment they would always go through the firewall. Additionally, the most sensitive part of the municipality’s security system is set up a bit more delicately whereby the user goes from server to server but also through the firewall.

‘’What is preventing (obstacles) municipalities of improving their chances against ransomware attacks?’’

As mentioned in the last paragraph, municipalities in the Netherlands are free to choose which security software or system they implement and from which supplier they get receive it. This means that municipalities do not necessarily use the same type of software or systems. When respondent 9 was asked if it would seem far more logical for them to use the same software to prevent ransomware attacks as it then becomes more manageable on a local governmental scale, respondent 9 answered ´I would agree with that, however I think it is a lack of central policy which makes it so that they do not use the same software´.

Respondent 7 believes that another obstacle which is preventing municipalities of improving their chances against ransomware attacks is due to there being a bureaucratic hierarchy within the organizations. He points out that the implementation or change in execution of certain things is far slower due to it taking so much time. Ransomware attacks can occur fast and in rapid succession; the time required to react to such an attack if the systems fail to is very little. Therefore respondent 7 points out that the administrative culture within the municipality will have to adjust to the situation in order to implement changes more easily in accordance with the situation.

Moreover, due to the budgets per municipality varying, the amount of funding put towards their cyber security will also vary. Respondent 7 supports this claim by saying ´And of course the budgets which vary in degrees are not always focused on security until the breach occurs´. Before the municipality of the Hof van Twente experienced the ransomware attack, no other municipality had experienced such an attack. After the ransomware attack however, other municipalities decided to take their security a lot more seriously due to the fear of also becoming a target. Respondent 8 believes that municipalities have to suffer a breach in order to realize just how unsecure their systems are. He pointed out that ´´If you really want to have a lasting effect then a breach has to occur at the organization´´. This claim is supported by respondent 3 which notes that the success of the ransomware attack at his municipality was due to the stupidities of the technical managers. Therefore, overconfidence in one´s cybersecurity is preventing municipalities of improving their chances against ransomware attacks.

‘’What sort of change would have to occur in order for municipalities to manage ransomware attacks more effectively?’’

Seeing as how municipalities have a bureaucratic hierarchy and certain decision can only be made by the higher ups change is not something that can happen on a whim. As respondent 7 pointed out ´´The administrative culture within the municipality will have to be adjusted in order to implement changes more easily in accordance with the situation´´. This however does not mean that the bureaucratic hierarchy within the whole municipality would have to be reorganized, as long as the individuals in charge understand that specific decisions with regards to change have to be made on a whim due to the

radical and unpredictable nature of ransomware the municipality's chance against such an attack could improve.

Therefore, a possible solution would be increasing the responsibility and authority of certain employees from the IT department which are trained to deal with such attacks and to take such choices depending on the situation. This will increase the implementation time of necessary changes and improve the municipality's chances of stopping the breach at an early stage.

Moreover, municipalities ought to reconsider just how much of their budget they are putting towards their cybersecurity. Some municipalities give the responsibility on spending the budget which goes towards cybersecurity to a IT-consultant who is either employed within the organization or hired from the outside. Respondent 2 who is employed at the municipality of Zutphen pointed out they give this specific IT-consultant the budget of 25 thousand euro's a year with the goal of spending the money towards providing the municipality with the best possible cybersecurity in any way he sees fit.

Not all municipalities chose this method as it would seem unwise to give one individual such responsibility. An example is the municipality of Zoetermeer which has a recurring budget and an annual budget. These budget plans are made yearly during which they decide what they will do the next year in terms of information security. Respondent 5 who is working at the municipality of Zoetermeer as an Information Security Consultant explained that awareness is very important and a recurring item. During the budget plans developments are looked at, what sorts of measures are in place, which are sufficient and whether adjustments need to be made. So in order for change to happen, budget plans on a yearly bases during which different experts are present might have a better impact than that of a single individual having the sole responsibility of distributing the budget.

''What are the costs and benefits of improving cybercrime prevention protocols?''

The beneficial impact which improved cybercrime prevention protocols can have on a municipality can make the difference between a successful and an unsuccessful ransomware attack. These improvements however can become costly both in time and money. The municipality of Hof van Twente for example has a yearly budget of 12 million euro´s which is meant to cover the municipality´s expenses on several different areas including cybersecurity. During their crisis phase of the ransomware attack the municipality had made 1.58 million euro´s worth of costs. After the ransomware attack however, an additional 2.32 million euro´s was spent in order to rebuild the breached systems. Respondent 1 pointed out ´´The financial loss was 4 million euro´s´. Not only does rebuilding the systems cost money, it also costs time and creates a delay in the work flow.

Respondent 1 further elaborated on this by saying ´´Our staff could not work due to not being able to log into their computers´´. Hof van Twente realized the importance of improving their cybercrime

prevention and had increased its budget towards rebuilding and improving their security. According to respondent 1, Hof van Twente is currently the most secure municipality in the Netherlands.

After the attack the Hof van Twente had decided to not change their security software suppliers except for one specific supplier which did system management for them. Respondent 1 explained that the reason for this was a discussion about how far the responsibility of a supplier goes which led to distrust between the municipality and this supplier. Afterwards, the municipality had decided to not extend the contract for the benefit of improving their cybersecurity. The relationship between a supplier and a municipality is one which is based on trust. Therefore, changing your supplier due to distrust means that a new supplier has to be found which takes up both time and money.

What is equally important to a supplier is a trained staff. Ransomware has many ways of breaching a municipality's system, but the easiest way is through phishing mails. These emails seem legitimate but they contain malicious URL's or attachments which will trigger the download of ransomware once clicked on right onto the system. If even one staff member would open such an email, the ransomware would spread rapidly through the network. When it comes to dealing with phishing mails however, knowledge is key.

Therefore it is pivotal to the improvement of cybercrime prevention that a municipality's staff is trained on a regular basis so that they are always aware of the different types of malware, the process of a breach and how it can be avoided works. Respondent 8 supports this claim by saying ''What you can do is organize roadshows, webinars or trainings to show them''. The municipality of Zoetermeer has been doing this with the goal of keeping their staff aware. According to respondent 5, the staff at the municipality visits the departments and give roadshows in various ways to keep them on their toes.

Conclusion

This research analysed which measures could be taken in order to protect municipalities from ransomware attacks. Four municipalities were selected based on their geographical location, whereby two municipalities came from the East side of the Netherlands and two came from the West side. This involved municipalities which had undergone a successful attack, a unsuccessful attack or had never experienced an attack before.

Chapter One covered the current landscape of the Dutch municipalities in the context of cybercrime attacks and in particular ransomware. The Dutch Data Protection Authority (AP) states that more than a fifth of data breach reports in 2020, came from the government, including municipalities. With the public sector's security not being updated fast enough the Dutch local governments cannot seem to keep up with the cybercrime being committed. The stolen data contain internal documents, including sensitive and confidential information between governments. Examples of these documents are personal details of executives, copies of passports and various agreements with foreign and local governments, and more specifically municipalities. The hackers demanded a ransom for the stolen information in return for these data.

Chapter Two discussed the routine activity theory (RAT) which helps analysing specific patterns of criminal activity at the macro and micro level through the evaluation of criminal trends. RAT can also be used to identify not just how criminal activities are perpetrated but to identify remedial mechanisms as well. For crime to occur, there must be three elements a motivated offender, an appropriate target and the lack of a competent guardian. In line with this, this research zoomed in on the municipalities that were attacked in the Netherlands. The municipalities Lochem and Hof van Twente have been targeted and successful attacks have taken place here. These attacks are enabled because of the increasing reliance of municipalities on computer systems and the internet on the one hand and on the other, technological vulnerabilities, fewer resources and lack of knowledge on how to defend against such attacks. However, Dutch municipalities still do not know how to appropriate detect and prevent such attacks. Studies on ransomware attack indicate three distinct steps in any ransomware attack prevention process which includes identification, prevention and response/recovery.

Chapter Three discussed the method of examination. This research uses a qualitative method during which current and former employees from municipalities and IT-experts were approached and interviewed. This research has attempted to produce internal assessments of the scope of impacts by assessing the impact of cybercrime attacks within the municipalities. A semi-structured interview is used for a better understanding of the answers and helped avoid possible ambiguities. Initially, the text fragments were analysed after which open coding took place. The first stroke involved open coding, where the arguments mentioned are dealt with. Next, axial coding was done to find out whether these are

mentioned more often by different respondents. From here it became possible to draw conclusions and identify possible connections.

Within the Netherlands alone millions of euros´ are involved so the impact can be quite comprehensive. An attack is most likely unnoticed and as soon as it is noticed, the damage is already done. There are enormous costs following the hack and hiring third parties. Besides the financial loss and possible image damage, there is also the delay in the work process. Employees cannot work due to computers that cannot be logged in. Reducing the number of attacks can be done by making the revenue model less lucrative for cybercriminals. It is important to take the right measures, especially in terms of prevention, and to have systems up to date so that they are not vulnerable and therefore an easy target for criminals. In the unlikely event that things do go wrong, it is important to be able to act quickly to keep the damage to a minimum. These consequences are related to the research question. The main question of this research is:

''How to improve cybercrime prevention protocols against ransomware attacks within Dutch municipalities?''

Cybercrime prevention can be improved by using a set of actions. These actions either complement each other or contribute separately to the bigger picture. It is important to have various mechanisms in place that actually detect, monitor and detect everything that happens in that network. In addition, protecting the municipality is a combination of various components, a so-called life cycle, of which prevention is one. Prevention as in drawing up a clear policy, increasing safe and aware behaviour among employees, taking technical measures such as end-point protection for anti-virus and anti-malware on systems, and mapping out risks and vulnerabilities.

First of all, it is important that the municipality makes its staff aware of cybercrime and ransomware in particular. Here, the consequences must be highlighted and how the chance of a ransomware attack can be reduced. After all, it cannot be ruled out that an attack will still take place. By means of workshops, webinars, roadshows and a training courses that is concluded with an examination, staff members could obtain a certification that proves they are capable of dealing with cyberattacks.

Municipalities have a unanimous strategy that they will not pay if such an attack occurs. Despite a lack of a central policy, all municipalities share the same approach. It is precisely the lack of a central policy that is striking and should be a point of attention. Entering into a joint venture between municipalities can ensure that software systems are purchased centrally and that similar structures are used. In this way, the SIEM SOC methodology could be deployed more broadly and, for example, regional or provincial monitoring could take place during which there is close contact with the IT experts of the municipality in question. After all, there are municipalities that have smaller budgets and cannot

afford to spend a substantial part on cybercrime prevention. It is precisely by sharing the costs (by rato) associated with cybercrime prevention that many municipalities can comply with security measures. In addition, municipalities can exchange experience that generally remain behind closed doors. It is precisely by exchanging this information that they can learn from each other and raise security to a new level.

Measures can also be taken within the municipalities themselves. Two-factor authentication is an example of this. By making this compulsory and using it within all applications, the chance of attacks is reduced. Currently, the municipalities investigated in this research utilize the Two-factor authentication method. However not all municipalities have applied it within all applications. This ensures that there are still openings for hackers to make use of it.

Moreover, the bureaucracy and administrative culture can increase the risk of attacks due to multiple links required within the process which can lead to vulnerabilities if the protocols are not followed. Having more steps within a process, could mean that at every step, something can go wrong. Setting up clear dummy-proof protocols, might seem like a solution. Improvement measures, however, need to be taken at multiple levels to achieve the maximum result of redundancy of protocols versus safety. Not having protocols and safety steps, will increase the vulnerability of the system, as will the increase of protocols and safety measures when they frustrate people in carrying out there day-today work. Both the internal and external changes will require time and patience, but the benefits will eventually prevail and the set of measures mentioned contribute to an improved security within municipalities.

Additional recommendations for municipalities

In the attack on the municipality of Lochem, it emerged that al relatively weak password “Welkom 2020” was used. Rules must be created for a password such as the use of upper- and lower-case letters, numbers and special characters. In addition, the use of network segmentation is recommended whereby a network is divided into different segments. By setting this up in this way each segment is acting as its own small network. The advantage of this is that network administrators and IT-experts are able to control the flow of traffic between subnets based on granular policies. This therefore makes it possible to identify irregularities more easily and timely.

As the COVID-19 crisis has led to more individuals working from home, the importance of working from home has also increased and this can also become a new target for hackers. Mobile devices have the same need for security as computers. With regards to protocols used within municipalities it is important to update computer and devices regularly. In this regard, security breaches in outdated programs or applications handled on mobile devices could be a possible gateway for hackers. Backing up data in different locations also enables municipalities to minimise disruption. The data can nowadays be

accessed from multiple places. If an attack is still successful, it is recommended to disclose it. This is the least damaging to the image.

Points of concern for governments

Having international cybercrime guidelines is recommended, whereby international law could be more useful and effective. Because attackers operate globally, it is sensible to address the issues involved jointly which could lead to international punishments for the same crimes whereby it does not matter in which country this takes place. In addition, the Dutch government can also endorse some practices through legislation. This may include the solutions mentioned in this research. For example, cooperation and exchange of data would then no longer be on a voluntary basis, but established on a legal basis.

Recommendations for future research

The results of this research provide insight into what organisations may be struggling with and show that progress can be achieved in this area. The results of this research show where the vulnerabilities are for municipalities. Research into the possible application of the SIEM SOC mechanism within municipalities has not yet been carried out. Follow-up research could focus on clustering municipalities where the SIEM SOC method can be applied. After all, the extent to which a municipality is an attractive target for hackers will vary according to its size. However, it is also important that small municipalities are not underexposed, because this involves sensitive (personal) data.

Currently, each municipality applies its own policy with regard to cybercrime prevention. Although it has been shown that cooperation brings financial and quality benefits, it is also important to find out how municipalities view this. This could therefore be a point for attention for future research.

Because this research has focused on four municipalities, it is recommended that a new cycle be subjected to this, in which several municipalities are included. This will give more insight and the possibility to generalise the results and to find out if the results relate to more municipalities.

It may also be interesting to work with behavioural scientists. After all, it has been shown that individuals are always the weak link and that access is gained through carelessness that can be traced back to them. Insight into human behaviour could therefore shed new light on the phenomenon of cybercrime and cybercrime prevention could therefore be based on behaviour as an additional angle. It can also be investigated to what extent other countries look at this and the best practices can be tested for possible application within the Dutch municipalities.

In possible future research, in which cross-analysis can be carried out, it can be examined whether the research results are comparable with the findings of the other researchers. Here, it can also be examined whether there are similarities for other municipalities within the Netherlands.

Limitations

This research can only indicate in general terms where cybercrime prevention needs to be improved. Due to the sensitivity of the subject, the researcher was not always able to obtain answers and information because this information could not be shared by the respondents. This includes budget issues along with the impact of a cyber-attack on working practices and internal protocols. Although this is not directly accessible to the researcher, the improvements brought up with regard to cybercrime prevention can then give direction to a further interpretation of this.

Although this research suggests possible solutions, the financial feasibility has not been examined. The recommendations show, for example, that cooperation in the area of cybercrime

prevention is the most sensible. If, for example, a SIEM SOC solution is chosen, this will also have budgetary consequences. Each municipality works with its own budget and it is therefore possible that a custom solution will have to be found for municipalities that do not meet these budgets.
Another important point is that hackers do not sit still in development. This research focuses on methods that are known today with regard to cybercrime prevention and ransomware. New developments in relation to hostage software, for example, could mean that the solutions proposed in this research become outdated over time or require additional modifications.

References

Adamov, A., & Carlsson, A. (2017). The state of ransomware. Trends and mitigation techniques. IEEE East-West Design & Test Symposium, 1(9), 1-8.

Akbanov, M., Vassilakis, V.G., & Logothetis, M.D. (2019). WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention, and Propagation Mechanisms. Journal of Telecommunications & Information Technology, 1(1), 18-24.

Akers, R. L. (2013). Criminological theories: Introduction and evaluation. Routledge.

Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security, 74, 144–166. https://www.sciencedirect.com/science/article/pii/S016740481830004X

Almashhadani, A., Kaiiali, M., Sezer, S., O'Kane, P. (2019). A Multi-Classifier Network-Based Crypto-Ransomware Detection System: A Case Study of Locky Ransomware. IEEE Access, 7, 47053-47067.

Alshaikh, H., Ramadan, N., & Hefny, H.A. (2020). Ransomware prevention and mitigation techniques. International Journal of Computer Applications, 177(4)), 1-20.

Ami, O., Elovici, Y., & Hendler, D. (2018). Ransomware prevention using application authentication-based file access control. The 33rd ACM/SIGAPP Symposium on Applied Computing. Pau, France, 1610-1619.

Atos (2021). Prevent ransomware attacks from taking down your business and defend your data. Atos, 1-10.

Authoriteit Persoonsgegevens. (2021, March 1). Cijfers datalekken 2020. Retrieved September 20, 2021, from https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-datalekken/cijfers-datalekken-2020

Authoriteit Persoonsgegevens. (2021a, March 1). AP luidt noodklok: explosieve toename hacks en datadiefstal. Retrieved September 12, 2021, from https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-luidt-noodklok-explosieve-toename-hacks-en-datadiefstal

Caporusso, N., Chea, S., Abukhaled, R. (2018). A game-theoretical model of ransomware. In: Proceedings - International Conference on Applied Human Factors and Ergonomics, Springer, Cham, 69-78.

Centraal Planbureau. (2019, October). Risicorapportage cyberveiligheid economie 2019. CPB.Nl. Retrieved September 10, 2021, from https://www.cpb.nl/sites/default/files/omnidownload/cpb-notitie-risicorapportage-cyberveiligheid-2019.pdf

Chen, Q., Islam, S. R., Haswell, H., & Bridges, R. A. (2019, August). Automated ransomware behavior analysis: Pattern extraction and early detection. In International Conference on Science of Cyber Security (pp. 199-214). Springer, Cham.

Choi, K. S., Lee, C. S., & Louderback, E. R. (2020). Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 27-43.

Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44, 588–608.

Connolly, L., Wall, S., & Oddson, B. (2020). An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. An Empirical Study of Ransomware Attacks on Organisations: An Assessment of Severity and Salient Factors Affecting Vulnerability., 6(1), 1–18. https://doi.org/10.1093/cybsec/tyaa023

Cooper, C., & Schindler, P. (2008). Business research methods McGraw-Hill: Boston. Retrieved on November 3, 2021 form, https://www.academia.edu/36184183/Business_Research_Methods_12th_Edition

Heppenhuis, M. (2021, October 14). *Cybercriminaliteit stijgt explosief in Oost-Nederland: 'Pakkans kleiner dan bij winkeldiefstal*. Destentor.Nl. Retrieved November 21, 2021, from https://www.destentor.nl/regio/cybercriminaliteit-stijgt-explosief-in-oost-nederland-pakkans-kleiner-dan-bij-winkeldiefstal~a1855743/?referrer=https%3A%2F%2Fwww.google.nl%2F

Foddy, W., & Foddy, W. H. (1994). *Constructing questions for interviews and questionnaires: Theory and practice in social research*: Cambridge university press. Retrieved on October 23, 2021 from, https://www.scirp.org/(S(i43dyn45teexjx455qlt3d2q))/reference/ReferencesPapers.aspx?ReferenceID=1681310

Glasser, D. (2015). A Routine Activity Theory-Based Framework for Combating Cybercrime. Igi-Global.Com. Retrieved October 10, 2021, from https://www.igi-global.com/chapter/a-routine-activity-theory-based-framework-for-combating-cybercrime/115771

Gibbert, M., & Ruigrok, W. (2010). The '"What"' and '"How"' of Case Study Rigor: Three Strategies Based on Published Work. *Organizational Research Methods*, *13*(4), 710–737. https://doi.org/10.1177/1094428109351319

Goyal, P., Kakkar, A., Vinod, G. & Joseph, G. (2020). Crypto-Ransomware Detection Using Behavioral Analysis Reliability, Safety and Hazard Assessment for Risk-Based Technologies. Springer Publications, 239-251.

Grant, L., & Parkinson, S. (2018). Identifying File Interaction Patterns in Ransomware Behavior. Guide to Vulnerability Analysis for Computer Networks and Systems. Springer, Cham, 14, 317-335.

Groenhuijsen, M. (2020). Ransomware. Een harde noot om te kraken. *Delikt en Delinkwent*, 2020(7), 513-527

Healey, M. J., & Rawlinson, M. B. (1994). Interviewing techniques in business and management research. *Principles and practice in business and management research*, *12345*. Retrieved on 3 November, 2021 from: https://www.bibsonomy.org/bibtex/1f09b49cc24a2755717dc9d04a21b969b/referrator

Hull, G., & Arief, J.H. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. Crime Science, 8(1), 1-22.

Kerner, S. M. (2021). Ransomware trends, statistics and facts in 2021. Retrieved from https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015, July). Cutting the gordian knot: A look under the hood of ransomware attacks. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 3-24). Springer, Cham.

Kılınç, H., & Fırat, M. (2017). Opinions of expert academicians on online data collection and voluntary participation in social sciences research. *Educational Sciences: Theory & Practice, 17(5)*, 1461-1486.

Kitteringham, G., & Fennelly, L.J. (2020). Routine Activity Theory. Handbook of Loss Prevention and Crime Prevention.

Kok, S., Abdullah, A., Jhanjhi, N., & Supramaniam, M. (2019). Ransomware, Threat and Detection Techniques: A Review. IJCSNS International Journal of Computer Science and Network Security, 19(2), 136-146.

Kuiper, J. (2020). Een verkenning naar de governance ten aanzien van cybercrime in Oost-Nederland."Want goede netwerken kunnen veel meer in de samenwerking".

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

Lovan, S., & Lovan, A. (2016). FROM CYBER THREATS TO CYBER-CRIME. JOURNAL OF INFORMATION SYSTEMS & OPERATIONS MANAGEMENT, 425–434. http://www.rebe.rau.ro/RePEc/rau/jisomg/WI16/JISOM-WI16-A15.pdf

Maiorca, D., Mercaldo, F., Giacinto, G., Visaggio, C. A., & Martinelli, F. (2017, April). R-PackDroid: API package-based characterization and detection of mobile ransomware. In Proceedings of the symposium on applied computing (pp. 1718-1723).

Ministerie van Justitie en Veiligheid. (2021, 3 mei). *Cybercrime*. Openbaar Ministerie. Retrieved on November 15, 2021, from https://www.om.nl/onderwerpen/cybercrime

Morgan, S. (2019). Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics. Cybercrime Magazine Cisco and Cybersecurity Ventures.

Nationaal Cyber Security Centrum. (2021, August 10). *Over het NCSC*. Retrieved November 20, 2021, from https://www.ncsc.nl/over-ncsc

Nauta, H., & Wheel, I. (2021, June 9). De overheid kiest voor makkelijke websites, niet voor veilige. Trouw. Retrieved September 15, 2021, from https://www.trouw.nl/economie/de-overheid-kiest-voor-makkelijke-websites-niet-voor-veilige~ba71a0b3/?referrer=https%3A%2F%2Fwww.google.nl%2F

Oerlemans, J. J. (2017). De Wet computercriminaliteit III: meer handhaving op internet. De Wet Computercriminaliteit III: Meer Handhaving Op Internet, 15(4), 350–359. https://scholarlypublications.universiteitleiden.nl/handle/1887/54783

Overheid. (1999, July 15). Kamerstuk 26671, nr. 3 | Overheid.nl > Officiële bekendmakingen. Overheid.nl. Retrieved November 15, 2021, from https://zoek.officielebekendmakingen.nl/kst-26671-3.html

Partida, D. (2021, August 31). *5 Reasons we're seeing more ransomware attacks than ever before*. AT&T Cybersecurity. Retrieved December 1, 2021, from https://cybersecurity.att.com/blogs/security-essentials/5-reasons-were-seeing-more-ransomware-attacks-than-ever-before

Pool, R., & Custers, B. (2017). The Police Hack Back: Legitimacy, Necessity and Privacy Implications of The Next Step in Fighting Cybercrime, European Journal of Crime, Criminal Law and Criminal Justice, 25(2), 123-144. doi: https://doi.org/10.1163/15718174-25022109

Reynald, D. M. (2011). Factors associated with the guardianship of places: Assessing the relative importance of the spatio-physical and sociodemographic contexts in generating opportunities for capable guardianship. Journal of Research in Crime and Delinquency, 48(1), 110-142.

RTL. (2021). Hacken ransomware defensive jusitie poltie losgeld. Retrieved on 8 December 2021, from https://www.rtlnieuws.nl/tech/artikel/5272070/hacken-ransomware-defensie-justitie-politie-losgeld

Ruffalo, J. (2021). Ransomware must be at the top of the administrative agenda. Retrieved from https://netherlandsnewslive.com/ransomware-must-be-at-the-top-of-the-administrative-agenda/259087/

Saunders, M., Lewis, P., & Thornhill, A. (2016). Research methods for business students (Seventh). *Nueva York: Pearson Education*. Retrieved on November 6, 2021 from https://www.pearson.com/nl/en_NL/higher-education/subject-catalogue/business-and-management/Research-methods-for-business-students-8e-saunders.html?tab=features

Saurbaugh, M., & Liska, A. (2017). Defending Against Ransomware with Intelligence, People, and Automation. Retrieved July 17, 2017, from https://goo.gl/6wRDwz

Shaukat, S., & Ribeiro, V. (2018). Ransom Wall: A Layered Defense System against Cryptographic Ransomware Attacks using Machine Learning. In: Proceedings - 10th International Conference on Communication Systems & Networks (COMSNETS), 356-363.

Shi, F. (2020, August 27). Threat Spotlight: Ransomware. Journey Notes. Retrieved November 20, 2021, from https://blog.barracuda.com/2020/08/27/threat-spotlight-ransomware/

Smaal, R. (2021). A method for secure distribution of confidential data to an untrusted environment. A method for secure distribution of confidential data to an untrusted environment, 1–12. https://www.naeon.nl/download/docs/naeon_paper.pdf

Surati, S. B., Prajapati, G. (2017). A review on ransomware detection and prevention. International Journal of Research and Scientific Innovation, 4(9), 2321–2705.

Tuttle, H., & Jacobson, A. (2019). ENEMY OF THE STATE: Ransomware Surges Against State and Local Governments in 2019. Risk Management, 66(11), 30-35.

Tyagi, M. (2017). Security against cyber-crime: Prevention and detect. Horizon Books (A Division of Ignited Minds Edutech P Ltd).

United States Department of Homeland Security (2020). Computer Emergency Readiness. Federal Government Resources.

Van der Sloot, B. (2017). De bevoegdheid van de politie om computers binnen te treden: tijd voor een grondrecht op de bescherming van informatie-technische systemen? Tijdschrift Voor Bijzonder Strafrecht & Handhaving, 3(4), 195–206. https://doi.org/10.5553/tbsenh/229567002017003004003

Van der Wiele, D. (2020, March 27). 'Cybercriminelen gaan voor het laaghangend fruit.' www.ccv-secondant.nl. Retrieved September 15, 2021, from https://ccv-secondant.nl/platform/article/cybercriminelen-gaan-voor-het-laaghangend-fruit

Verhoeven, N. (2014). Wat is onderzoek? (5e druk). Den Haag: Boom Lemma. Retrieved on November 16, 2021 from https://hhs.bibliotheek.budh.nl/boek/9789059316713/#:~:text=De%205e%20druk%20van%20Wat,methoden%20en%20technieken%20van%20onderzoek.

Wecksten, M., Frick, J. Sjostrom, A., & Jarpe, E. (2016). A Novel Method for Recovery from Crypto Ransomware Infections. Springer, 1354.

Wikström, P. O. H. (2009). Routine Activity Theories. Oxford Bibliographies Online Datasets. Published. https://doi.org/10.1093/obo/9780195396607-0010

Winter, R., Ruiz, R., Army, B., & Archer, R. (2018). Cyber Autoimmune Disease When the Virtual Life Imitates the Real Life. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 7(1), 21-30.

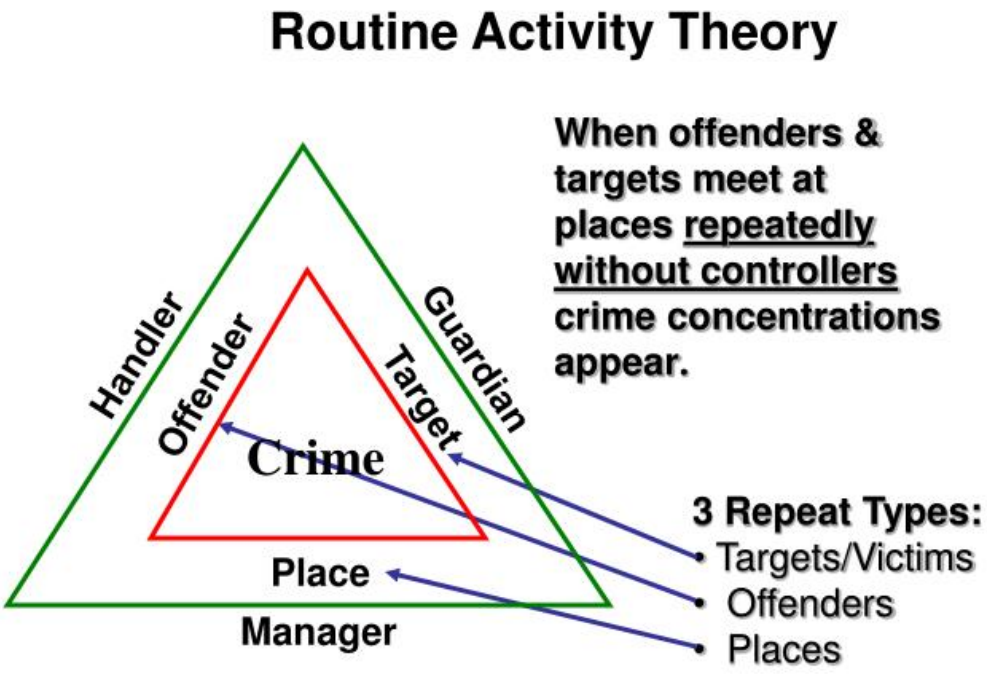
Wolf, J. (2018). Ransomware Detection. Friedrich-Alexander-University Erlangen-Nuremberg.

Zavarsky, P., & Lindskog, D. (2016). Experimental Analysis of Ransomware on Windows and Android Platforms : Evolution and Characterization. 94, 465–472.

Zimba, A., & Chishimba, M. (2019). On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems. European Journal for Security Research, 4(1), 3-31.

Zimba, A., & Mulenga, M. (2018). A Dive Into the Deep: Demystifying Wannacry Crypto-Ransomware Network Attacks Via Digital Forensics. International Journal on Information Technologies & Security, 10, 57-69

Appendix I - Routine Activity Theory



Appendix II - Information Form

Dear Sir/Madam,

As agreed, you will receive information about the interview on <date>.

This mail contains information to give you an idea of the subject matter, to give you ample time to gain knowledge of the investigation, and to facilitate the interview process. With regard to this interview, the conditions are as set out in the AVG regulations.

Topic

The scope of this investigation is cybercrime and in particular ransomware. For the sake of completeness, these two terms will be described so that there is no ambiguity about the context of this study. Cybercrime can be defined as a criminal act where hackers break into a computer and/or computer network. Ransomware is a malware category that exploits security mechanisms such as cryptography in order to hijack user files and related resources and demands money in exchange for the locked data.

Due to the increasing threat of ransomware attacks and the need for insight into this, it is a challenge for many municipalities to better manage their IT infrastructure and make maximum use of it. Part of that challenge can be addressed by looking at municipalities where there have been both successful and unsuccessful attacks. This will provide insight into the case. Since you are employed by the municipality, I would like to ask a few questions in order to provide information that can be used in finding possible links. At the moment, no study has been conducted that investigates this within Dutch municipalities. This research is therefore aimed at filling the gap in the literature.

The questionnaire below provides insight into the questions that will be asked during the interview.

1. How would you describe cybercrime and are you familiar with the definition of ransomware?

For the quality of the answers it is important that the respondent has knowledge of the criteria. This question is used to check whether the respondent has fully understood the information form. Asking this question can remove possible ambiguities.

2. What is your role within the municipality?
3. How long have you been active within the municipality?
4. Have you ever experienced a cyberattack within your municipality?

Yes (1)

-How did the municipality act here?

-To what extent has the municipality suffered a loss?

Yes (>1)

- Have you also seen possible patterns in different attacks?

No

- If you have not, can you imagine what risks there might be for the municipality?

6. How is cybercrime prevention currently organised in your municipality (infrastructure)?

- Which system is used?

7. How is cybercrime prevention currently organised in your municipality with regards to budget and policy?

-Do you have insight into the costs associated with cybercrime prevention and weighs this up to the possible benefits?

8. Are cybercrime prevention methods and information being shared among municipalities to your knowledge?

9. Has your municipality adopted an infrastructure or strategy with regards to cybercrime prevention which is also being implemented at foreign municipalities?

10. What could be done to prevent possible attacks in the future?

-Do you have any specific examples (e.g. at a previous municipality or employer)?

Important point of attention

Prior to the interview, could you find out which system or systems your municipality uses with regard to cyber-crime prevention (e.g. Citrix)?

I would like to thank you once again for your cooperation.

Kind regards,

B. Faraj

Appendix III - Consent form

Research project: **Cyber Crime prevention within Dutch municipalities**

Researcher: B. Faraj

- I've been briefed on the investigation. I have read the Information Form for which has been sent prior to the interview.
- I was given the opportunity to ask questions about the investigation prior to the interview.
- I have been given the time to decide whether to participate in this study.
- I consent to the use of the data collected during this study for the purpose of this scientific research and I may revoke this consent at any time.
- I understand that any information I provide in relation to this study will be collected anonymously and will not lead back to me or to my organization and person (AVG-regulations apply).

In order to participate in this research, please sign consent form below. If in any case you would disagree with the points above feel free to withdraw.

Participant

Name:
Date:

Signature:

Researcher

I declare that the participant mentioned above has been informed of the above investigation both in writing and orally.

Name:
Date:

Signature:

Appendix IV – Coding Scheme

Resp.			
	Fragment	**Open Coding**	**Axial Coding**
Resp. 1	The hackers got in after 100,000 automatic attempts via a programme that cracked the password so that they were in the system within three weeks. If the password had been more difficult it would have taken half a year but they would still have got in (if there was two factor security they would never have got in). Once inside, it was just a matter of shutting the door and no one could enter the system anymore. Policy-wise they have different rules, everyone has to change their password, use authenticators etc.	Weak password	**Two-Factor authentication**
Resp. 1	Image damage was not calculable, because they were transparent to the public, this damage was reduced.	Transparency	**Limited image damage**
Resp. 1	financial loss was EUR 4 million (budget is 12 million a year)	Financial	**Financial damage**
Resp. 1	cannot work due to computers that cannot be logged in.	Work disruption	**Delay**
Resp. 1	(Municipalities work together with suppliers on the basis of trust, they used to use Citrix but now another system is used. The attack was not successful because we happened to use Citrix, but because our password was too weak, so after 100,000 attempts in 3 weeks they got into the system. After the attack the municipality chose to work with other suppliers and they have become a lot more critical)	Proportions	**Confidence**
Resp. 1	(After that successful attack, the municipality increased its budget so they are now rebuilding their security from the ground up, which will make them the most secure municipality in the Netherlands.	Budget planning	**Increased budget**
Resp. 3	don't do anything stupid, make sure you have sufficient audit and control in place so that people who are experts and procedures that conform to best practices are looked at again	Procedures	**Audit and control**

Resp. 1	Passwords should be changed at regular intervals and not be easy ones like your mother's name or pet's name with 123 behind it. Since the hackers often acquire programs on the dark web that just go through all the numbers and letters before they get the right password, it is therefore very important to also use two factor authentication, because only this will prevent the hacker from getting through to the system.	Security	**Two-Factor authentication**
Resp. 2	I don't know how they got the case where you log on to Citrix and then there's a firewall behind it and they didn't get through that.	Firewall	**Firewall**
Resp. 7	As far as I know, that's not really possible at the moment. And you always have to have your question or your technology that you want to use continually checked as municipalities because problems also develop. You still need to be able to add or adjust certain systems based on the problems or issues you have as a municipality. So you'll always have people to do that for you that can system maybe partially automatic but not always one hundred percent.	Control	**Audit and control**
Resp. 2	Actually, we did, because when we found out that someone had gotten into them on that Citrix NetScaler, which is what that thing is called, okay, then it set off all the alarm bells for us.	Citrix NetScaler	**Alert system**
Resp. 2	We are affiliated with the Information Security Service (Informatiebeveiligingsdienst), an organisation that is based on the Association of Netherlands Municipalities (VNG), and they monitor all kinds of things, so they monitor our traffic, but they also warn about critical patches.	monitoring critical situations	**Information Security Service**
Resp. 2	We have, however, tightened up the testing policy	Testing	**Increased testing policy**
Resp. 2	We do invest in awareness on an ongoing basis, and one of the things that was done recently was that all personnel had to take a kind of exam preceded by video workshops.	workshops	**Staff training**
Resp. 2	But what I said was that 25,000 a year is something he can spend himself on things he needs, and it's separate from the preservation budget. We also have an education and training budget that is at group level and covers everything.	Budget planning	**Increased budget**

Resp. 2	People who don't pass that test really have a problem so you can retest it again, that's all right and you can watch all those videos again, that's all right	Quality Staff	**Staff training**
Resp. 2	Well, Lochem is also tested, but it is up to you to decide how to implement this testing, for example, the Jericho principle that it has there, not everyone or segments or so, but two factor authentication, for example.	Security	**Two-Factor authentication**
Resp. 2	Yes, it is the number one protector of citizens' data That is, if you don't do that yet If you don't do that well That is bad for your image	Security	**Limited image damage**
Resp. 6	I saw such a beautiful video on YouTube of a cat going over the norm below the norm behind but that's what users do, you don't think of it but they do. And yes, these users will work around measures because technically they can do a lot but people should be able to continue to do their work and not be burdened with them. In fact it should be invisible and at the end of the day the user is the last one to click on something or to be approached by telephone, so a lot of attention should be paid to the soft side, without being pedantic.	measures	**Background measures**
Resp. 2	I have that hanging on him yes it depends a bit on how much it costs I would say but that damage well if really the whole thing is encrypted and you and you can't do anything anymore	Cost and benefits	**Cost-benefit analysis**
Resp. 2	Yes, that certainly happens, the F&G organises all kinds of conferences and I don't know what else, and for example, the municipality of Lochem has learned from its lessons and I would like to share those lessons with them, so they do indeed make various appearances left and right to introduce themselves, from where things went wrong, but also what has been done well to make it miss a few things well done to begin with	Conferences	**Information exchange**
Resp. 2	But you also had it foreign, no that is not the case at all. We do not copy from abroad	Structure	**No foreign input**
Resp. 2	I do see something nationally organised SIEM SOC that all municipalities are behind. That is, the active monitoring of entry and exit traffic by specialised parties	SIEM SOC	**National organised system**

Resp. 3	What we tried to do was to see if from the back up if the operational servers and databases et cetera could be restored but they found out pretty quickly that yes the only backup there was apparently accessible from our own domain	Backup	**Backup issues**
Resp. 3	We scaled up and called in a meeting with a party with professional networks to deal with the breach. In this case the NFIR and a kind of colleague of FOX with FOX being a well-known one. But there's also NF4 which we asked.	Meetings	**Collaboration**
Resp. 3	But that was actually very quickly decided that they were just not going to do anything about it, eh, from the principle that as a government you can't do it yourself, you can't morally afford to go into business with criminals, so it was a principled decision not to deal with the ransomware threat because of extortion and to take the situation as it arose for granted and to see how we can move on.	Confidence	**Zero trust computing**
Resp. 3	Well, doesn't make much sense to try to keep this under wraps for a long time because within a week the news will have leaked out again. You need to hire all kinds of people. I know that the estimates of what it costs exactly depends a bit on what you include or exclude as a consequence of the damage.	news	**Openness**
Resp. 3	But we don't actually have our own premise infrastructure anymore, we use the services of IaaS	Infrastructure	**IaaS**
Resp. 3	In the play offs but some that are important in that reasonable for the best practice, moreover we are on the I don't know if you ever heard of it but it's called the zero trust computing.	Infrastructure	**Zero trust computing**
Resp. 3	Zero trust computing is actually the approach you have to choose the moment you build your own infrastructure and outside your own environment. That means that we for example have a on our endpoints on our laptops we have certain software that detects strange behaviour that that same software that we also have in the spotted server so the moment the service starts to show weird behaviour or starts to communication with foreign destinations or that the foreign script tries to run unauthorized scripts it will be blocked or it will be signalled to the administrator	Infrastructure	**Zero trust computing**

Resp. 3	Everyone who does something with us now is doing it because you see there are also a lot of software vendors who have to install or configure systems, and yes, that's all no longer allowed with generic accounts or via a TeamViewer session. People who have to have such accounts must all be given access to the VPN and environment with a special management server and so on	Security	**Additional security**
Resp. 3	Well the systems we used were pretty much the same, however what we did do is add a number of additional security components which we didn't have before. Before that we didn't have real cows and point protection and we also didn't have a number of components to monitor the behaviour of the servers and to report to a SIEM SOC situation. But these are indeed additional software components that you use in the context of information security, but in my opinion it doesn't cost you that much	Security	**Additional security**
Resp. 3	We had Citrix yes but that Citrix didn't play a role in the way it came about directly uh the way they got in is really a fundamental or two or three fundamental errors because on a server which for legitimate services used the internet connection to the outside and on that server the RDPORT the remote desktop port was just exposed to the internet so that means it's actually a firewall configuration error	RDPORT	**Firewall configuration**
Resp. 3	That server was accessible and the password of the local department it was the brute forcing that means it's just that and that server was not zoned and the password of a local department was brute forcing that means that the server was actually accessible	Accessibility	**Server weak spot**
Resp. 3	It has actually not much to do with Citrix and all that stuff it has actually to do with all the respect stupidities of the people who are technical managers with us today I can't call it otherwise.	laxity	**Human inadequacies**
Resp. 3	Yes absolutely because if you would have had that then it would have been virtually impossible for that to happen because then a brute force attack makes no sense.	Security	**Two-Factor authentication**

Resp. 3	because of a number of other incidents, a kind of joint service was set up under the VNG. It is called the IBD, the Information Security Service for Municipalities, with the aim of, say, raising the level of knowledge development in the municipality and they also try to stimulate the exchange of knowledge and skills between the municipalities themselves.	Exchange of knowledge	**Information Security Service**
Resp. 3	If you say risk management is chance of something happening times effect If you see that this results in a fairly large chance with an enormously large impact, then the answer is: "That's the start of the business case to take measures against this in order to get that security up to a high level and everything stands or falls with that.	Security	**Two-Factor authentication**
Resp. 3	because of a number of in my view rather stupid mistakes that it went wrong where people did not understand sufficiently that what they were doing constituted a risk and apart from that we also had nothing in place to detect possible intrusions or to be able to detect hacked systems so you know	knowledge	**Lack of knowledge**
Resp. 1	No, each municipality has its own budget that it spends on its own software or prevention methods. Municipalities do not share methods or information with each other	No information sharing	**Own policy**
Resp. 3	I have spoken to quite a few people from the municipal information security sector and in all honesty I have to admit that they are not at the level which is actually the minimum level on which you can say that you are doing things right and yes, that includes SIEM SOC.	SIEM SOC	**National organised system**
Resp. 3	if you want to fill in the SIEM SOC and you have to do all sorts of things yourself because with all the positives you have to analyse whether it is a real one or a false positive	SIEM SOC	**National organised system**
Resp. 3	I think that it is one of the measures that should be in place nowadays. The interesting thing is that a few years ago we from the VNG (Vereniging voor Nederlandse Gemeentes) participated in a tender in which SIEM SOC was to be implemented.	SIEM SOC	**National organised system**

Resp. 4	I think there's a lot of money risk involved in that which I did understand in a cybercrime e-learning I had to do in my first week i learned that this is really a problem in the Netherlands alone about millions of euro´s are involved what's being made out so I know what kind of impact it can have.	Financial	**Financial damage**
Resp. 4	Yes we have a VPN which is switched on when working from home or when you are on a different network than the municipality itself and for the rest they let everyone do e-learning now and then on the things you should pay attention to in order to prevent cyberattacks.	e-learning	**Staff training**
Resp. 4	Yeah, we use a two factor authentication app sometimes but mostly to log into our own remote systems and I am not aware of any other systems using it.	remote systems	**Two-Factor authentication**
Resp. 4	Yes, in any case, the e-learning I think that goes through an external party that offers that so there will be money they are spending money on that for sure however in terms of policy i do not really know myself.	Budget planning	**Unknown budget**
Resp. 4	No, I don't known but I wouldn't expect them to because it would probably cost more to do that instead of applying Dutch protocols.	Cost and benefits	**Less costs**
Resp. 4	Well first of all make sure all your employees are aware of the importance of good passwords and a good VPN and that you do not do strange things on public Wi-Fi networks and also anyway the physical security even when you for example tail gate which is when people walk behind you through a gate or something with an excuse you should just be alert as an organization.	Awareness	**Staff training**
Resp. 5	Yes, the pattern is actually generally that either an attempt is made on the front or on the outside, so to speak, a scan is made to see if they can get at something. Well, that is generally pretty well secured, and we also have a service that monitors that 24/7. But the pattern you see is that when a cyberattack occurs, it is often via the user or the employee that the entrance is found to entice something or to click on a link or an attachment and gain a foothold that way.	employee	**Attack via employee**

Resp. 5	I know we made the news once, I think it was the local part of the AD, when it was about your um failure card. It was an initiative that is now called Basisbeveiliging.nl and they do a scan, I think, of all public organisations such as central government and municipalities, I think, water boards as well. And they look at what kind of visibility an organisation has on the outside of the internet and how they deal with certain standards. The teles institutions, things like that, so that's how we've made the news on occasion, but not shy of a criminal activity.	Reliability	**Reliable image**
Resp. 5	Certainly because our town clerk also wants to propagate the fact that we, as a government organisation, also have the task of being a reliable government organisation	Reliability	**Reliable image**
Resp. 5	No we have a similar environment then via VM ware is that, so the user uses a local workstation and a virtual workstation that virtual workstation is actually always when you log in a fresh workstation and when it logs out it is destroyed. We use a number of standard security measures, such as not being able to install software just like that, and we use security software that is located in both the Microsoft 365 section, and therefore in the Cloud section and on the workstation and that's a combined system, so it's not two separate systems where I have to look for problems because they communicate with each other.	Infrastructure	**Centralized systems**
Resp. 5	We have also divided the network into compartments, so that means that if I go to my server environment as a user, I actually always go through the firewall and in the sensitive part of our system and actually our most important applications there, we have set it up a bit more finely whereby I go from server to server also through the firewall.	Protection	**Firewall configuration**
Resp. 5	Two factor we do have on our cloud services that anyway and on the phone and on our Cloud applications but internally we don't have that.	cloud	**Two-Factor authentication**

Resp. 5	It depends a bit on where, in my opinion, at Hof van Twente it had to do with an RDP machine which they had hooked up to the internet and, well, we try to learn from incidents like that. For example, if you look at the Hof van Twente, what we did was to look at how big the risk is that when we connect a server to the internet, we have exposure in that way, and what we agreed with our firewall service is that if there is a rule whereby a machine is directly connected to the internet, a signal goes out anyway saying, are you sure you want to set this rule?	Protection	**Firewall configuration**
Resp. 5	We also looked at recovery procedures, so if you assume that you have a problem, how are you going to repair it and how are you going to limit it. In any case, by segmenting we are trying to limit this in this way and in addition we looked at our back-up procedures and I think we have been working on this for a year now in order to really print byte and to get it sharper and to merge it more because each discipline often had its own procedure. And we are also working on our own backup location at a municipality site.	procedures	**Own backup location**
Resp. 5	No, there is indeed a recurring policy or budget, yes there is an annual budget, annual plans are made, so each time we look at what we are going to do next year in terms of information security. Awareness, for example, is an important and a recurring item, and we also look at developments, so to speak, and whether the measures we have now are sufficient or whether adjustments need to be made.	Budget planning	**Fixed budget**
Resp. 5	The funny thing is that on the one hand, the administration says: yes, we want to be back online as soon as possible so that we can serve our citizens and entrepreneurs again, so the payment is probably on the table, but the pros and cons should be weighed. But on the other hand, the Public Prosecutor's Office, the IBD and the VNG (Association of Netherlands Municipalities), I believe, also advise against payment. On the one hand, this is a very brave decision and a very principled one, and it may also be a sign that municipalities do not allow themselves to be extorted, which makes them a less attractive target.	Cost and benefits	**Cost-benefit analysis**

Resp. 5	If you look at a healthcare institution or hospital, for example, they can't afford to say 'we're not going to pay, we're going to rebuild the entire environment in a month or two or three', so they may be more inclined to pay and are therefore a more attractive target. A fundamental consideration would be no, we won't do that and we trust in our measures. I think that would also be an important point: how big is the damage and can you repair it or not? And if you are in a completely different position: I cannot repair it, what do I do now? And then you have to pay, which by the way is not a guarantee that everything will be released by the hackers.	Status quo	**Cost-benefit analysis**
Resp. 5	I think it's admirable how open they've been about this. I sometimes use the example of 'if you suffer damage to your image, you will be the example in various presentations in the coming years'. I think Maastricht University did the same and so did the municipality of Lochem. This gives an insight into how a process like this works and why I think it's a good thing, but it does take courage to act this way as a municipality.	openness	**Limited image damage**
Resp. 5	Well, the only thing I can think of is zero trust, which is a strategy in the field of infrastructure, and that is something we have indeed adopted and are trying to apply, and it has even been made compulsory for government institutions in America, I believe, but that is something we have been doing for a long time.	Infrastructure	**Zero trust computing**
Resp. 5	It is actually very easy to uh carry out such an attack and also the chance of being caught or convicted for this is of course very low so yes the risk for an attacker is just very low and therefore very interesting.	Infrastructure	**Zero trust computing**

Resp. 5	If you see what is being earned, especially with hostage software, but I think that 10 years ago, hostage software was seen as something annoying and of which you had a single machine that encrypted files, but now it takes down the whole organisation, and there are very professional organisations behind it that have much more time and now also, as far as I am concerned, much more money to do this sort of thing, and once again the chance of being caught is very low. And behind them there are huge organisations that have much more time and, by now, much more money to carry out these kinds of activities.	Budget planning	**Increased budget**
Resp. 5	Yes and what other colleagues of ours also do is visit the departments and yes give roadshows in various ways.	Roadshows	**Staff training**
Resp. 5	Yeah absolutely I mean look SIEM SOC is something that uh what is coming up more and more but just connecting to a SIEM SOC is not a solution in itself. With us we see that on our firewall service as well that's kind of a stripped down SIEM SOC but specifically focused on our infrastructure and our firewall. With SIEM SOC, of course, you link even more log sources and get even more signals, and then you have to make use cases for okay, when do I want to be alerted, when do I not want to be alerted, because there is just a lot of information coming out and there is the risk of false positives, so a false alarm is just very high, but it can certainly contribute to discovering what is deviant, I think that is the most important thing, so what deviates from the norm and what is different from normal.	SIEM SOC	**National organised system**
Resp. 5	Well own specialists in this area is just very difficult because the professional SIEM SOC is also looking for these people and yes whether you can work for a cool idea company or for a municipality there is probably a difference in pay and I think if we would have a SIEM SOC specialist that would be attracted very quickly by other municipalities or companies.	SIEM SOC	**National organised system**
Resp. 6	To my knowledge, we have not adopted anything specific from foreign municipalities.	Structure	**No foreign input**

Resp. 6	Of course, we all work on the basis of the BIO, which stands for baseline information security for the government, and we are supported in this by the information security service, which also acts as a sectoral CERT, or Computer Emergency Response Team, and through them we do receive all your reports, so we also receive more information from the Hof van Twente in this way. So that's how you should follow that line. But there's a lot in there about fitting in, so you can look if you think it's a good plan and you're considering doing something completely different.	Government support	**Information Security Service**
Resp. 6	I think you have to keep helping your employees to make the right choices and actually what we are mainly doing is making sure that somewhere in the back of someone's mind there is something that makes them think that maybe this is not a good thing and that they ask for it. When we do roadshow workshops, we try to get people to be alert in that way and hope that they don't do it and ask first and that we can help them further. And these roadshows seem to help enormously because we also do our best by being creative, for example today we made a Sinterklaas poem which is about that, so just in a playful way because otherwise it quickly becomes playing police and you don't want that because people are inclined not to report anything out of fear. You have to tell them in a playful way and yet very clearly what they really shouldn't do and that helps. I always give the good example that someone who works in IT can get things a lot closer, but 100% safe is of course a utopia and people can continue to work so it shouldn't take an hour,	workshops	**Staff training**
Resp. 2	There are guidelines that are similar, but the municipality ultimately makes its own choices	guidelines	**Own policy**

Resp. 7	Well, a municipality is actually a very juicy target for cybercriminals. Because all the data of all the inhabitants of a particular municipality is contained in it, I think, just about everything. It may even be because the central system has been found with perhaps other types of systems, such as the tax authorities' financial data and things like that, so yes, it is very attractive and it is also very essential to what municipalities do, so yes, they have to implement a certain policy and if that information is not available for a certain resident or for a certain thing, then it is very difficult to do their job.	Information	**Load of information**
Resp. 7	Well I actually think it's due to different factors, so cybersecurity is not just typing a few codes into the terminal and you're in. That's what we call layered security and we strongly recommend it to our clients, so not only on a technical layer but also on your processes. If your processes are not good you can have problems and someone can use that. Because it doesn't necessarily have to be an external person, sometimes it can also be an internal person, which we call insider threats, but also, for example, the people themselves, so you can have the best systems, but if your people don't know how to use them or how to use systems safely, then that's a very big factor as well.	**Two-Factor authentication**	**Two-Factor authentication**
Resp. 7	Image damage is very difficult to express in money at billion, that's actually what they call risk management so how much risk do you have and what are the consequences of such risks but yes according to GDPR is I think off the top of my head 8% or so to your annual turnover at large companies yes then I think that has a lot of impact of course.	image	**Limited image damage**
Resp. 7	True, but what they often do is calculate how much do I have to spend as a company to do disaster recovery and the criminals want to use an affordable amount so they know for sure that companies have something like I would much rather pay than have to do disaster recovery.	Cost and benefits	**Cost-benefit analysis**

Resp. 7	Yes, I have used it myself in the past and yes it is actually the case with different kinds of cloud-solutions. You see, for example, a very big trend towards the cloud and you also see, for example, remote desktop, that kind of solution. And if a company or a municipality chooses to manage everything itself, then of course there are certain things that come with that, so I'm actually quite neutral about the use of the cloud.		
Resp. 7	As far as I know, at least the last time I was on the radio, the Tax and Customs Administration uses about 900 systems on average and these are usually external systems which they purchase from I don't know which one and the government which works for certain municipalities in cases of the public sector, so yes, but these can also be real commercial applications. But nowadays you can see, and I can say this with certainty, that they mainly manage part of it themselves on their own servers, for example by exchanging files and things like that, if they have on-premise servers there. But that would also be purchasing a lot of software or purchasing various things from the Cloud or other SAS solutions.	policies	**own policy**
Resp. 7	Yes two factor authentication is not a bial solution for all cyber-attacks, so only a piece of the puzzle but a very important piece of the puzzle if you have two factor authentication you can set up different things as a company so for example a company can look from where certain login attempts are made that can be based on that code but also based on location so in principle it is a very important solution but as I said it is a piece of the puzzle.	**Two-Factor authentication**	**Two-Factor authentication**
Resp. 7	Yes, in principle, as a municipality you have to map out the indication landscape very clearly, so like a lot of what they call Shadow IT, things that are used but that you don't know are used, for example, a user giving an employee a Dropbox account somewhere or a group of people for a particular project having a Dropbox account somewhere.	Map out	**Overview**

Resp. 7	But actually yes cybersecurity is actually a cycle like process so you need to be able to continuously kind of map out the different threats you need to be able to come up with appropriate solutions for them and this is how you actually continuously strive to improve your security posture.	ongoing	**Ongoing process of security**
Resp. 7	So how security-proof you are actually is usually not done in municipalities, which is partly due to the nature of the problem. For example, commercial companies are generally much quicker at adopting certain things, but because there is a whole bureaucratic hierarchy within municipalities, the implementation of certain things or changes or the execution of certain things is much slower because it takes so much time. Perhaps they can also do something about that kind of administrative culture so that certain things are implemented much more easily and, it's actually a complete package so you actually have to look at what the threats are, what can I do about them and how can I improve myself as a municipality.	Rules	**Bureaucracy**
Resp. 7	I don't think it's black and white that just buying software has its disadvantages, but doing everything yourself also has its disadvantages. If you do everything yourself as a local authority, then you have to have a separate ICT department which is responsible for creating and maintaining software for you 24/7, for keeping your systems up to date and for improving them, so each local authority would then have to have its own IT department. But if you also purchase everything, then the monthly costs will also pile up, in my view as a local authority.	Security	**Increased security measures**
Resp. 9	No, they all use different ones this is to be very little at the wave standardisation among municipalities.	different software	**Own policy**
Resp. 8	to hack into security systems and to tell the client what can be improved upon security wise so we hack into the system and tell the client these points are very badly secured we advise you to fix them.	Pen testing	**Professional hacker**

Resp. 8	Yeah that's the point, you have to create backups to restore security. What i mean by that is ransomware usually spreads on the networks, so you need to have a strong network segmentation.	Backup	**Own backup location**
Resp. 8	What that means is when you have production service on host A network A and a production service on host B network B, the service of A and B should not reach each other unless they need to do so.	Separate networks	**Separate networks**
Resp. 8	But in case its a new ransomware type which is not yet known that other than isolating the infected host and cutting everything off is to make sure to save the devices which are the least likely to get infected.	Infection	**Isolation**
Resp. 8	But what i noticed is that they were using the exact same encryption algorithm, and other patterns I cannot really think of any right now.	Pattern	**Identical encryption algorithm**
Resp. 8	well to be honest ransomware attacks are happening more everywhere and that's because it's quite easy.	Relatively easy	**Increased attacks**
Resp. 8	But for the public sector it may have to do with the systems being old or the staff is untrained to handle ransomware attacks.	old systems	**Outdated systems**
Resp. 8	but if you were to send that same mail to a municipality where the staff is untrained and has no knowledge on the phishing mail then it is far more likely that the email will be opened	Lack of knowledge	**Lack of knowledge**
Resp. 8	Exactly, that would be far more effective than just telling your staff about it. But the problem with that is that from my experience with banks mostly is that they hire penetration testers only to receive one report from the tester which states that their security is up to par with the standards so that they receive a certificate, or something instead being continuously kept up with.	Pen testing	**Professional hacker**
Resp. 8	I mean you can do is create roadshows, webinars or trainings and show them	Workshops	**Staff training**
Resp. 8	My senior colleague told me how 10 years ago there was no cybersecurity expert team or penetration testers because there was nobody who believed that they would be needed.	security team	**Increased security measures**

Resp. 8	The same has to happen with a municipality, so what you can do is to keep everybody informed and keep testing them by sending fake phishing mails or use fake breaches to keep them on their toes.	Workshops	**Staff training**
Resp. 8	The next thing we can implement is end point security. For example when you see a file enter someone's computer with an unknown signature just block that file	End point security	**Increased security measures**
Resp. 9	didn't react until the information became public which is unfortunately the way a lot of people get the incentive to start looking seriously at security once it be made public they started I had to look for solutions protections for their networks data.	image	**Limited image damage**
Resp. 9	The risks are pretty high because of course municipalities have a lot of information about the citizens and that should be predicted on the GDPR or AVG and it is proving a difficult subject for lots of municipalities	Information	**Load of information**
Resp. 9	If I just briefly cover commercial organisations, commercial organisations concentrate on enough turnover to make enough profit and they see security purely as a cost if we talk about municipalities this looked at differently that they have a budget which is this has to be spread thinly over all there it	Cost and benefits	**Cost-benefit analysis**
Resp. 9	and again because people seem to believe that by putting a single firewall in the network they have good protection and by using antivirus software on endpoints they have good protection they leave it at that until they find that they do get a cyberattack.	Firewall	**Firewall**
Resp. 9	One is specific for the IBMI platform and that is actually a unique product at the moment at least for the IBMI platform in discovering and preventing ransomware from attacking system and the other product which we sell which has a specific module for ransomware it's called trap X	Software	**recognition software**
Resp. 9	I think it's a lack of central policy which makes it so that they do not use the same software.	lack of policy	**National organised system**

Resp. 2	Then we locked the whole thing up, so that it was no longer possible to work from outside, for example. We had a lot of home workers and now that was no longer possible and that caused damage.	permanent work environment	**Restrictions work process**
Resp. 9	Well again it's missing the central overseeing point which commercial organisations will have within their organisations	lack of policy	**National organised system**
Resp. 9	and of course the budgets which vary in degrees are not always focused on security until the breach occurs.	Cost and benefits	**Cost-benefit analysis**
Resp. 9	conference which is held in normally would be held in Utrecht on the yearly basis and there is a combination of a trade exhibition and conference.	Exhibition	**Information exchange**
Resp. 9	I think awareness is the main thing because it acts can come in from all angles and a lot of attacks coming through phishing attempts via end uses PCs and that way they get into the network of the municipality so it's really important I think to make note on of the stuff more aware of the dangers but also every year every employee which has an an endpoint should also be made aware of the dangers	Awareness	**Staff training**
Respondent 10	we also hired a forensic IT-company pretty who immediately saw that things were going wrong and together we carried out a number of analyses and had to establish that we really had to start building rebuilding the complete environment again	Forensic team	**External knowledge**
Respondent 10	Well, in any case it has been a very difficult start to the school year for the employees, all the preparations, everything that you have ready, you can no longer use. So there is always some financial damage	delay	**Financial damage**
Respondent 10	also some damage to image. But getting hacked is becoming more and more normal and yes, it's also about how the press deals with it.	image	**Image damage**
Respondent 10	there are just enormous costs following the hack and hiring third parties.	costs	**Financial damage**

Respondent 10	which then need to be purchased new as well as new service firewalls and that is quite a pricey operation.	new services	**Firewall**
Respondent 10	Yes it does because rebuilding our systems we chose to immediately strive for a higher level of security moreover, several things need to be considered such as investments in your suppliers, external parties and stuff needs to be reinstalled	higher level of security	**Increased security measures**
Respondent 10	I think that there is a set pattern but it really deepends on the situation. Also because how you were hit, how your back-ups are, how valuable the data is and how much insight you have into the data that is out in the open	Same orders	**Same pattern**
Respondent 10	There are often so many files that the analysis is not made quickly. The extent to which you are affected and how bad that is for a company depends on so many factors that there is very little that can be said in general terms about this.	Environment	Lack of clarity about consequences
Respondent 10	Now that we have done more than we did before, we have, say, really introduced end-points and MFA for students as well, and even better forms of end-point security, but we have also introduced a further form of network segmentation	End point security	**Increased security measures**
Respondent 10	and an internal firewall, which means that you are better protected on several levels.	Firewall	**Firewall**
Respondent 10	Yes, we already had two factor authentication for employees and we have now also introduced it for students.	Two-Factor authentication	Two-Factor authentication
Respondent 10	This is often done on the basis of functionality and you arrive at one or more suppliers who can offer this and, of course, we also make demands. Suppliers who meet those requirements and can offer the functionality are the ones we choose. And if a tender limit is exceeded, a choice is made on the basis of the suppliers, often looking at SLA and alike.	agreements	**SLA**

Respondent 10	The software security budget has been raised somewhat. I also think it is necessary because the outside world is just the way it is. When we now acquire the new software packages, the security bar will immediately be raised again, so I think it will grow a little in the organisation, so it's not as if the budgets for software are going to be raised very, very high at once, specifically for each package.	Budgetplanning	Increased budget
Respondent 10	Yes, I think that sometimes municipalities want too much of everything, especially when you look at local governments and the tax money that we spend, but apart from that, from a security point of view, one and one is much more than two, so the moment you start working together on that, and dare to make choices, together you can create a much safer system with much more security because you're all working on the same principles	Collabaration	**National organised system**
Respondent 10	And if you start to see this more as a utility, then it is easier to explain that you can use the same thing together. Because yes, of course, everyone has their own wishes, but all the processes are basically the same, so you would have to weigh up user convenience versus security and also make a business case for it, and yes, I think I know which way that would fall.	Same procedures	**National organised system**
Respondent 10	Well if you don't pay, you will undermine the whole businessmodel at a certain point, because if you don't pay, you will have to do it all together, and that, there is also something in return, unfortunately, that sometimes privacy-sensitive data is out on the street, no matter how annoying that is. That is the consideration that a society will have to make, but the moment you start protecting those important data more effectively, the chance of losing them will be smaller. So if you are already hacked into, that kind of data cannot be hit easily, that is a quick win I think we should work on together.	Better measures	**Increased security measures**

Respondent 10	Well as I said, on several levels, because if more and more parties decide not to pay, then it will be less lucrative, because it takes a lot of effort sometimes to prepare it properly for such a group. On the other hand, you can never prevent it, so you have to secure your entry points properly, really secure them with two factor authenticatio		
Respondent 10	and a good password policy, and be able to explain that well to your users, combined with the right behaviour, how do you deal with data and therefore dare to take decisions as an organisation	policy	**Own policy**
Respondent 10	And a bit of network segmentation and that together will never prevent it, but it does prevent the big leaks. So if we invest in that, I think we're already well on our way.	network	**Increased security measures**
Respondent 10	Yes i am aware of SIEM SOC, but there are a number of preconditions. I think it can help, but it has to be active enough for organisations, because that's where it often goes wrong. Certainly a SOC can take a lot of the hassle out of having those specialists apparently in a certain number of places. And then you have to think very carefully about the organisation around it, what processes and agreements you make so that it will provide real added value. I certainly believe in that, because that is the efficient use of scarce knowledge and resources, but then you have to implement it very well.	Siem Soc	**National organised system**
Respondent 11	And then what we did was we immediately formed a team of four people to focus on that case so you have multiple hands and eyes and can give people various tasks. The most important thing was that we managed to disconnect the system from the internet so that no further damage or direct influence was possible. Then we immediately went into communication with the customer to give instructions on what we thought the customer should or should not do next.	communicating	**Communication**

Respondent 11	We have had several cases so the exact impact and damage has varied over the times we have had it but actually it was in all cases. Image damage is a funny thing and so you ask image as a question and it really depends on the company how public it is and especially the semi-governmental organizations also sometimes have functions that can take place more in the background. There, of course, the image case is less direct. What did happen over the years was that companies became subject to obligations in connection with the AVG Act, so in that respect an obligation to report arose, and you could see that as a kind of image damage, so they are on the list.	image	**Limited image damage**
Respondent 11	You are actually hit unnoticed and as soon as you notice it, the damage is already done because as soon as you get a message, because that is one of the next steps in the process that you are asking about	unnoticed	**Financial damage**
Respondent 11	But I think some companies have no choice and that's not just because of the image damage but purely because they don't have enough money to pay that ransom. So if I summarize, I would say that there are 3 factors that play a part in that consideration, from ethical to economic to image	costs	**Cost-benefit analysis**
Respondent 11	, I interviewed the hof van Twente local authority and they said that because they were transparent with the public about the attack, they suffered much less damage to their image.	Transparency	**Limited image damage**
Respondent 11	, the municipality has personal data, and depending on the content of the data, you could say that all the residents have been informed, and that it is transparent, which means that the damage to the image of the government body is limited. But it can also contain data that is personal to all those residents and therefore causes prohibitively high damage.	Transparency	**Limited image damage**

Respondent 11	I think it's fair to say that 90% of them are poorly set up for this. You asked about the word infrastructure, so the technical side of the story was, of course, partly our responsibility, as we were the infrastructure managers. But even if we had everything in order, there was still a layer of behavior from our customers' employees and yes, I can almost say that in almost 100% of the cases, people did not handle security well.	behaviour	**Lack of knowledge**
Respondent 11	A lot of them just worked in the office and they didn't have to deal with Citrix at all or not always I should say. And the small organizations just have a standard network without Citrix-like solutions. But in the course of 30 years more and more people started working from home and working from the internet became more and more popular. In addition, e-mails have also become more and more common. In fact, all the attacks that we have had, I think, have occurred via e-mail where users have clicked on links that they should not have clicked on.	behaviour	**Lack of knowledge**
Respondent 11	But I think I can say two things about this, my feeling is that we were actually always working on it, on how do you ensure that the infrastructure is securely closed, and of course we often had enough back doors that we discovered too late. But actually, hacking did not occur too often from that side, so it did happen, and we did have attacks from outside, but actually, with normal management, that always went well.	Secure infrastructure	**Increased security measures**
Respondent 11	So the other side is that we also trained people to know about cyber attacks, but then to really get it to a manageable level for the users is the hardest part in my experience.	training	**Staff training**
Respondent 11	But I will mention a more complicated route, but it is available: suppose you have a central system where you share data with people	central system	**Centralized systems**

Respondent 11	a lot of people just use Microsoft OneDrive. Or Google-like system and now they just put data on there, and then they have two factor to get in or not. But then they share it with people who don't have two factors and you can't see that. You can't say 'I only want to admit people who have really good security'. But the incidents that we have had were also at a time when the security was less strong, for example Microsoft is now paying attention to this.	Two-Factor authentication	**Two-Factor authentication**
Respondent 11	Yes, but you have to learn to pay attention to it as an infrastructure manager and you also have to train the users to demand from their parties with whom they share data that they in turn also have sufficient protection from their side	train	**Staff training**
Respondent 11	It has to do with the fact that in the Netherlands there is no fixed policy for municipalities regarding security software or systems.	No fixed policy	**own policy**
Respondent 11	It depends on the budget of the municipality, so each may use a different system or software. I have interviewed the municipalities of Hof van Twente and Zutphen and they both had Citrix as their system during the attack.	Costs and benefits	**Cost-benefit analysis**
Respondent 11	If you notice that Citrix is not watertight, you can simply investigate and say, okay, we will exclude Citrix from use. But Citrix is not sitting still either, they know in no time where their weak points are and will of course close them solidly. Then you get an attack from another type or another brand. So whatever software you choose, you will always have to set up a system where you say there must be an overarching controller system that keeps an eye on the packages.	Security	**Increased security measures**
Respondent 11	And last year, I think, there was an attack via that management software, so that has nothing to do with Citrix, which the client had chosen, but with the management software we had chosen. So, we also had to choose at a certain moment that we would switch to another management software. And in the end, we	Security	**Increased security measures**

	decided to keep the same software because that company took the necessary measures to close the security gaps		
Respondent 11	Well, in any case, they are responsible for taking the right measures, so it wouldn't be wrong if the suppliers had a certificate or a rating and they could show that they follow and know the right procedures. So that's not to say that there is a package and that package is not satisfactory, but you must constantly look at whether the packages are used or chosen, as you gave as an example Citrix. You simply have to attach a certificate or a control system that says that everyone can be hacked at some point or a hole can be found.	**Specialized teams**	**Specialized teams**
Respondent 11	if they manage it together, the advantage is that they can exchange data with each other about numbers and about leaks that have been found. But I don't think it necessarily has to be a municipality. There are now more and more developments that cyber security companies and authorities in the Netherlands that are concerned with cyber security are paying more and more attention to it centrally and are exchanging information with each other about it.	information	**Information exchange**
Respondent 11	So don't place the responsibility with municipalities and also not only with the suppliers of that software. But with a central system that does this for the whole of the Netherlands across all packages.	Broad responsibility	**National organised system**

Respondent 11	So I don't think you have to do it on one IT-company or one package, but that it really has to be a joint effort of several companies that agree with each other that you just have to work together on this. Because on the other hand, coming back to your question, municipalities have certain considerations as to why they opt for such a policy or not. That is often not very convenient for the budget.	Collabaration	National organised system
Respondent 11	Well I think you've mentioned a few things like two factor seems to me a mandatory thing to have.	Two-Factor authentication	Two-Factor authentication
Respondent 11	So for municipalities, too, just as you appoint a personal datamanager for the AVG, I think it's useful to appoint a team and say you are responsible for the cybersecurity of this municipal institution.	Specialized teams	Specialized teams
Respondent 12	We have quite a few measures in place to ensure that if we are attacked, we can detect such things. For example, last year we worked with a chain partner of ours where a workplace had actually been hacked into and from that workplace 400 people in our organisation had been contacted with a phishing mail	Alert	Alert system
Respondent 12	It was so good and so legitimate that it got through all those systems, and that created a lot of work, especially for us, to approach all those 400 people personally to ask if they had left their data or changed passwords. But because we saw all this happen quite quickly, we were also able to respond very quickly and we also saw exactly who had received the new phishing e-mail and who had, as it were, clicked on the link it contained. So as far as that's concerned, that's very nice, because that's another cyber-attack and of course they come in all shapes and sizes.	alerts	Alert system

Respondent 12	Only to the extent that the systems needed for the municipality's business operations to work could not be used. Especially the fact that it takes a lot of work to check that everything is working again, that we can trust that nobody has entered their password somewhere, but that it is not because we have been taken hostage afterwards.	delay	Increased security measures
Respondent 12	Cybercriminals always make use of (globally) known vulnerabilities in systems, the fact that there are so many attempts to detect them makes it clear that they continuously scan the infrastructure and systems of companies and organisations for these.	Attempts	Professional hacker
Respondent 12	Failure of crucial systems and therefore the continuity of primary processes, data leaks, image damage in the municipality is a party that is trusted by the citizens. Very specifically, well, I don't know if you've been following the news over the past week, but you should take a look at it. There's a vulnerability in Java, which is present in just about every system and device used in the world, and that means that there are also municipalities, including Hof van Twente, which have already shut down their services.	image	Limited image damage
Respondent 12	. It is quite intense, and yes, there is a risk involved, and they know better than anyone what that risk is - look and they are an example, so maybe that is a bit of a negative approach, but for many other municipalities, no one wants to go through that experience of not being able to provide your services to customers for two or three weeks and losing your data. After all, as a municipality you want to be reliable for your citizens, so the last thing you want is not to be able to deliver. People who die and people who are born cannot be registered, you cannot apply for driving licences or passports and you cannot arrange parking permits, it's all very wide-ranging.	delay	Delay

Respondent 12	If you compare this to five years ago, when companies were still ashamed if they were hacked, and nowadays it only helps if you are transparent, because then others will help you sooner and your image damage is indeed much smaller, look, the credo nowadays is not whether you are hacked but when you are hacked.	Transparency	Limited image damage
Respondent 12	. We have switched to a new workplace but there is still Citrix in the underlying infrastructure but that is not really a security measure. The Citrix is more of a tool. And you can't protect yourself against cybercrime, because it's just there, but you can prevent malicious parties from getting into your network and we have set up measures for that, such as a SOC service and a Security Operations Centre which monitors on the outside whether strange things are happening, where people are trying to break in or that certain systems are being broken into or log in attempts are being made to see if people or someone can get in	SOC	National organised system
Respondent 12	So, we have various mechanisms in place that actually detect, monitor and detect everything that happens in that network. In addition, protecting the organisation is a combination of various components, a so-called life cycle, of which prevention is one. Prevention as in drawing up a clear policy, increasing safe and aware behaviour among employees, taking technical measures such as end-point protection for anti-virus and anti-malware on systems, and mapping out risks and vulnerabilities	prevention	Increased security measures
Respondent 12	By detection, I mean a SOC-SIEM solution that detects suspicious traffic flows from the Internet and on the internal network. Detection through the preventive measures taken, for example the actual detection of a virus. And response, which stands for the ability to respond quickly to a report/incident by applying the Security Incident Process.	SOC SIEM	National organised system

Respondent 12	That depends, because the VNG (Association of Netherlands Municipalities) has a website called the IBD, which is the information security service, and it contains a lot of information about how things are organised within municipalities, but also about the general threats to municipalities, and it also gives examples of how you can do it	VNG	Information Security Service
Respondent 12	this organisation also supervised a tender called GGI Secure, which is a kind of generic infrastructure. The idea was to buy these kinds of products for many municipalities at the same time so that all the municipalities could use them. Look, some municipalities have a whole team of experts who have experience with this and understand how it works, but a lot of municipalities also have someone in my position who is available one day a week, you know. Because it is then mandatory, someone is appointed or someone who used to do the bookkeeping is appointed as CISO yes that is not someone who understands cyber security.	Scarcity	Lack of knowledge
Respondent 12	Yes, we have a new workplace now because many people work from home and that includes it anyway, and before that it was always set up for people who worked remotely. So, it was always impossible to work from home with a token or with a code in the phone. In addition, administrators use this as standard for logging in, and SAAS applications are used more often, and we mainly use SSO because, I don't know if the term means anything to you, but it stands for Single Sign On, which is linked to your workplace account and which remembers your passwords, so you don't have to use separate passwords everywhere but that is already a kind of secure link	Security	Increased security measures
Respondent 12	You can then use your workplace login details to log into such an application and if that is not possible with one supplier, for example, then MFA two factor authentication is the minimum requirement to have.	Two-Factor authentication	Two-Factor authentication

Respondent 12	But what I just said is that the level of knowledge of the people is also very different in all municipalities, and not everyone has the money to put experts in place and arrange that, but of course we have the information security service, which also has a CERT, so you can call them if you have a problem and they will collect the information for all the municipalities, so you can fall back on them if you are hit by a cyber-attack.	Information Security Service	Information Security Service
Respondent 12	But what is still lacking, for example, is a governmental obligation, which you now see increasingly frequently in companies, that you are obliged to arrange certain things and that you can also be fined for this if you cannot demonstrate that you have your security in order. Because nowadays, of course, there's still a lot at stake, and there is at organisations that are part of the vital infrastructure, such as Schiphol Airport or the harbours or the energy supply, but it doesn't apply to municipalities yet. And your question was whether there should be one; I think there should indeed be one and that you should enforce it even if it's a long	Lack of obligations	own policy
Respondent 12	We have insight into the costs involved in preventing cyber incidents. This is actually a sum of various factors and the technical and organisational measures taken. This certainly outweighs the benefits. For example, in the case of a ransomware attack, an organisation must deal with ransomware (which government bodies usually do not pay on principle) and high recovery costs, especially if the ransom is not paid, it may be necessary to rebuild systems completely.	Costs and benefits	Cost-benefit analysis
Respondent 12	Yes, there is a lot of attention for information exchange. In particular, the information security service of VNG plays a major role here. For example, a number of years ago there was a tender with which municipalities could purchase preventive technical security products. In addition, the IBD supports with various security products such as handbooks an exemplary approach and supports when an organisation is hit by a cyber incident	Information	Information exchange

Respondent 12	Strategy and measures against cybercrime are in many cases based on international norm frameworks, standards and global best practices. Dutch municipalities must comply with the BIO (Baseline Information Security Government). This government-wide framework of norms is based on the international ISO270001/2 standard for information security. A municipality abroad may have to comply with a different national framework of norms, but it will always be based on international best practices.	Baseline information security government	Internation best practices
Respondent 12	Yes, look ultimately if you have set up a SOC-service then it is so that you can react to it. If you are attacked, then you can see it and then you can react to it. It's just like a burglary in your house, if you have your window open and your doors open and your neighbour has everything locked and barricaded, then yes, they won't go into your neighbour's house, they'll go into yours. And it works the same way with a cyber-attack because hackers scan the network all day long to see where there are systems with doors open that have vulnerabilities and yes, if they pass by your organisation and your systems are not vulnerable and they are up to date, then yes, they will go to the neighbour and if they do have a vulnerability, they will hack them. So, SOC is one of them, so it monitors and can react if things go wrong, but it is much more important to make sure that you are not the candy shop for a hacker and that they come and look at you.	SOC	National organised system
Respondent 12	So preventive, and that has to do with prevention in technology, so keeping your systems in order, but it also has to do with your employees understanding what they have to do, so that they shouldn't just click on anything or share everything with everyone, and that's a very wide range, of course. In addition, cyber-attacks cannot be prevented, they will always occur and are expected to	Security	Increased security measures

	increase. Reducing the number of attacks can be done by making the revenue model less lucrative for cybercriminals. It is important to take the right measures, especially in terms of prevention, and to have systems up to date so that they are not vulnerable and therefore an easy target for criminals (after all, burglars also choose the house they can get into easily or where there is something specifically to gain). In the unlikely event that things do go wrong, it is important to be able to act quickly (incident response) to keep the damage to a minimum.		

Appendix V – Coding Variable List

Appendix VI – Interview Request Letter

Dear Sir/Madam,

As a master student of Public Administration at Leiden University, I hope to conduct research this year as part of my thesis on how different municipalities in the Netherlands deal with cybercrime and cybersecurity. This research will be conducted under the supervision of Professor Matt Young. More specifically, with this research I want to find out how local governments define cybercrime and cybersecurity, what forms of cybercrime they have experienced within their organization, what kind of damage this caused and what they do to protect themselves.

As part of my thesis research I am looking for IT experts who work in this field. My question is whether there is room within your municipality to provide me with information by conducting an interview of 20-25 minutes. The interview does not focus exclusively on policy staff in your municipality, if there are experts in the IT department I would be happy to hear from them.

I sincerely hope that you as a municipality would be willing to cooperate. If you would like more information or can help me further with this question, you can always reach me via email: bawanx@hotmail.com or phone: +31619990300.

Thank you for considering this request.

Best regards,

Bawan Faraj