Critical Decision-Making in Time of Crisis

DEALING WITH TARGETED RANSOMWARE

Bhaskar Dercon | 1514687 | Master Thesis | 31-07-2020
University supervisor: Dr. Els de Busser
Second reader: Dr. Tatiana Tropina

As part of a graduate internship at Fox-IT
Internship supervisor: Diederik Perk, MA

Table of Contents

Introduction

1.1 A Christmas extortion....3

1.2 What's happening?....5

1.3 Research aim and strategy....6

Methodology

2.1 Introduction....8

2.2 Research scope....8

2.3 Literature study and conceptualization of variables....8

2.4 Survey....9

2.5 Questions....10

2.6 Target population....10

2.7 Sampling strategy....10

2.8 Distribution....11

2.9 Data analysis....11

2.10 Limitations....12

Literature and Conceptualization

3.1 Introduction....14

3.2 (Targeted) Ransomware....14

3.3 Targeted ransomware as organizational crisis....15

3.4 Decision-making during organizational crisis....16

3.5 The Framework....17

3.6 Micro Dimension....18

3.7 Meso Dimension....18

3.7.1 Strategy....19

3.7.2 Structure....20

3.7.2.1 Structure: Hierarchy and Authority....20

3.7.2.2 Structure: Economic Incentives....20

3.7.2.3 Structure: Communication Systems....21

3.8 Macro Dimension....22

3.8.1 Institutions 22
3.8.2 Stakeholders 23

Analysis of Results

4.1 Introduction 24
4.2 The dataset 24
4.3 General considerations about ransomware 25
4.4 Ranking the considerations 28
4.5 Structural interpretation of results using the theoretical framework 30
4.6 Meso dimension 30
4.6.1 Strategy 31
4.6.1.1 Statistical significance 33
4.6.2 Structure 33
4.6.2.1 Structure: Hierarchy and Authority 33
4.6.2.2 Structure: Economic Incentives 35
4.6.2.3 Structure: Communication Systems 40
4.7 Marco dimension 42
4.7.1 Institutions 43
4.7.2 Stakeholders 44
4.8 Conclusion of chapter 45

Conclusion

5.1 Introduction 47
5.2 To pay or not to pay 47
5.3 Recommendations 50

Bibliography

Bibliography 53

Appendices

Appendix 1: Terms and conditions survey 57
Appendix 2: Survey questions with translation 58
Appendix 3: T-test sectorial comparison 63
Appendix 4: Targeted ransomware decision tree 65

Introduction

1.1 A Christmas extortion

It is almost Christmas as crisis hits at Maastricht University (UM). On the evening of 23 December 2019, system moderators employed by the University find themselves locked out of their systems and notice that a big part of the Universities IT service has stopped working. Responding to the incident, the IT security team quickly discovers that a large part of their Microsoft Windows infrastructure is locked and that services like email and student portals are not accessible.[1] The security team quickly realizes that this incident is not the result of misconfigured software or a human error; it seems that the University has been hacked. And while on any given day the UM fights of more than 1200 digital intrusion attempts, it appears that this one has been successful and that the intruder has spread ransomware, a kind of malicious software which encrypts all the data on the systems it is employed on, making the systems inaccessible and de-facto useless without a working decryption key. With this realization, the security team concludes that the UM is in serious trouble and that external professional help is needed. The same night a call is made to FoxCERT, the Computer Emergency Response Team of Dutch cybersecurity vendor Fox-IT.[2]

The next day a team of experts from Fox-IT is dispatched to the scene to aid the emergency effort. They are tasked with advising the crisis management team and start a digital forensic investigation into how this attacked happened and what can be done to mitigate its effects.[3] The same day the media catches wind about the story and reports stating that Maastricht University has fallen victim to a ransomware attack are starting to surface.[4] With this, the University realizes that external communication about the crisis is essential as students and employees need to know what is going on, and because the systems are locked, it is not possible to send them an email. The decision is made to use the website of the University, which was not affected by the attack, as the primary portal to communicate with the external world. The same day a statement is posted.

> 24 December 2019
>
> **Cyber attack against UM**
>
> **Maastricht University (UM) has been hit by a serious cyber attack. Almost all Windows systems have been affected and it is particularly difficult to use e-mail services. UM is currently working on a solution. Extra security measures have been taken to protect (scientific) data. UM is investigating if the cyber attackers have had access to this data. It is unclear how much time UM needs to find a solution, but it will definitely take a while for the systems to be fully operational again.**
>
> **All UM buildings are closed until Sunday, with the exception of the research labs at UNS 50.**

The team tasked with technical analysis of what happened quickly discovers that the UM has become a victim of a specific ransomware strain dubbed Clop ransomware, which had previously hit Antwerp University.[5] The assessment that it was indeed Clop is made by because the files encrypted by the ransomware had a *.clop* extension, and a file called *ClopReadme.txt* is found. The file is a digital ransom-note and states instructions on

[1] Maastricht University, 'Cyberaanval - Een Samenvatting'.
[2] Mathijs Dijkstra and Maarten van Dantzig, 'Spoedondersteunig Project Fontana'.
[3] Mathijs Dijkstra and Maarten van Dantzig.
[4] 'Universiteit Maastricht kampt met ransomware-aanval'; 'Groot Cyberhack Bij UM'; 'Ransomware Infecteert Systemen Universiteit Maastricht - Security.NL'.
[5] 'Universiteit Maastricht kampt met ransomware-aanval'.

how to get in contact with the attackers.[6] The message is pretty clear: if you want your systems back online and don't want to risk the loss of any files on the compromised systems, get in contact with us. From this moment on the UM is faced with a dilemma, it is clear that they are dealing with a criminal group that is trying to extort them: are they going to get contact with them to find a solution for their problem or will the UM decide that it does not negotiate with criminals?

At the same time, a broad crisis management operation is set up. More than 200 UM employees are called upon and come to work during their Christmas holiday and work around the clock to resolve the crisis; among them are IT-employees, helpdesk staff, communication advisors, facility staff, and, of course, the senior management.[7] The downtime of the IT-services and the reports of a ransomware attack has made students and researchers anxious. They wonder: is my thesis stored on the university network safe? I need to graduate next month, is this still possible? Are the exams planned in two weeks still taking place? I have sensitive research data stored on my university work environment, has this data been compromised? And that moment, two days into the crisis, the UM is unable to answer these questions, there is still no clear idea of which systems have been compromised and all the IT-services, except the website, remain offline.[8] The executive board is faced with a difficult dilemma that needs choosing: are they going to get in contact with the hostage-takers, see what their demands are and possibly pay the ransom demand or are they going to start an operation to restore the systems themselves and work with Fox-IT to see what data can be saved?

Both options are defined by great uncertainty in terms of outcome, and both options have their ethical implications. First of all, paying the ransom takers doesn't guarantee that your files will be decrypted. Although threat actors employing ransomware indeed have something to gain by keeping up a reputation that shows that they indeed will decrypt the files after payment, this is not a guarantee.[9] Furthermore, paying ransom means that you are sponsoring a criminal enterprise that will use this money to attack others and continue their felonious business model. Going in the other direction and decide to start an operation to restore the compromised systems without decryption keys provided by the attackers also has its implications. The University could try - maybe with outside help - to decrypt the files themselves. However, the chance of success of such an undertaking is uncertain, to say the least. Furthermore, such an operation would be a timely undertaking, leading to prolonged downtime of the University's IT-systems. Given its uncertainty, this option poses ethical implications as well. What if students are not able to graduate because their master thesis has gone into thin air or an important research project has to be restarted because it was on one of the compromised servers? Additionally, what would be the legal implications of failure in this scenario, could the University be sued for negligence?

After careful deliberations, it is decided that the possibility of losing vital data together with long sustained downtime of the University's IT-systems would be an unacceptable risk to take. What could have played a role in this decision was the fact that the threat actor behind the attack was identified as TA505, a known and financially motivated criminal group that has been active for some time. In earlier attacks of the group, they had indeed provided decryption keys after payment, and even though this still did not give total certainty that the attacker would indeed provide working decryption keys, it was decided that this course of action would have the highest chance of success and would thus be best for the University, its students and her employees.[10] After contact was made with the attackers using email, it becomes clear that the ransom demanded is 30 Bitcoins,

[6] Mathijs Dijkstra and Maarten van Dantzig, 'Spoedondersteunig Project Fontana'.
[7] University of Maastricht, 'UM Cyber Attack Symposium – Lessons Learnt'.
[8] 'Update: Cyber Attack at UM #2'.
[9] Cartwright and Cartwright, 'Ransomware and Reputation'; TechRadar and 2016, 'A Helping Hand with a Dirty Trick: Ransomware Now Offers Helpdesk to Victims'.
[10] University of Maastricht, 'UM Cyber Attack Symposium – Lessons Learnt'.

around 197.000 Euro at that time.[11] On the 30th of December, the payment is made, the same day the decryption keys are provided, and the University can start its recovery process. The recovery process takes time and is intensive, but on the 6th of January, when the Christmas holidays are over, the university can start-up operations as they would normally do. And while some IT-services are still unavailable or somewhat unstable, there is no data loss, exams take place as planned, and students are able to graduate in time.

1.2 What is happening?

The scenario above is what can be described as what cybersecurity researchers have dubbed 'big game hunting,' a practice in which criminal groups target organizations with sophisticated cyberattacks to spread ransomware, lock the organization's systems and subsequently extort them for large sums of money.[12] Cybersecurity vendor Coveware calculated that the average ransom demanded in targeted ransomware scenarios in Q1 of 2020 was around $111,000. With this being an average and actual demands going as high as a few million, it is safe to say that the business model of targeted ransomware is a very lucrative one.[13] In their target selection, the criminal groups employing this business model have been indiscriminate, and without any restraint, as they have been targeting almost every kind of organization one can imagine. Hospitals, government institutions, municipalities, emergency services, research institutions, high schools, factories, universities, fortune 500 companies, insurance providers, dental clinics, oil refineries, and even veterinarians have fallen victim to their malicious practices.

The direct costs and economic impact attached to these attacks are hard to measure in a truly academic fashion. The number of victims is high, their organizational profile distinct, the impact per case differs, and only a fraction of cases are revealed publicly. Furthermore, it is difficult to make an economic assessment of the impact a ransomware attack has on external stakeholders like supply chain partners or customers. However, cybersecurity vendor Emsisoft has triangulated data from different sources to create a picture of the economic impact that is related to ransomware. It should be noted that cost estimations provided by commercial cybersecurity vendors should always be taken with a grain of salt because their business model stands in direct connection with the figures they put out. However, the Emsisoft calculation is transparent in its considerations, assumptions, and data gathering process and can, therefore, be useful in giving some insight into the scope of and the cost connected to the topic presented in this research.[14] However, even if the figures shown in their calculation are inflated, the results presented here are quite overwhelming.

Total cost: ransom demand costs + downtime costs (16 days)

Country	Total submissions	Minimum cost (USD)	Estimated cost (USD)
United States	24,770	2,324,912,200	9,299,648,800
Canada	4,689	440,109,540	1,760,438,160
Germany	10,688	1,003,175,680	4,012,702,720
UK	4,999	469,206,140	1,876,824,560
France	8,754	821,650,440	3,286,601,760
Australia	2,874	269,753,640	1,079,014,560
Spain	8,840	829,722,400	3,318,889,600
Italy	11,580	1,086,898,800	4,347,595,200
Austria	1,698	159,374,280	637,497,120
New Zealand	467	43,832,620	175,330,480
Global total (all countries)	**452,151**	**42,438,892,860**	**169,755,571,440**

[11] University of Maastricht.
[12] 'Internet Crime Complaint Center (IC3) | High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations'.
[13] 'Ransomware Payments Up 33% As Maze and Sodinokibi Proliferate in Q1 2020'.
[14] 'Report: The Cost of Ransomware in 2020. A Country-by-Country Analysis'. For a detailed overview see: https://blog.emsisoft.com/en/35583/report-the-cost-of-ransomware-in-2020-a-country-by-country-analysis/

Ransomware poses one of the biggest cybersecurity challenges of today, an observation shared by both cybersecurity professionals and law enforcement. The business model is highly costly and highly disruptive to the organizations it targets and poses serious consequences for external stakeholders. There are lots of variables that define the characteristics and the severity of a ransomware scenario: what is the scope of the attack? Are there vital systems compromised? Are there still back-ups available? What is the amount of ransom demanded? Is their critical data stolen? Is the organization experiencing downtime? Does the attack threaten the business continuity of the organization? And so on. However, if a ransomware attack is successful, meaning that critical systems have been compromised and recovery operations to back-ups or decrypting the files without the help of the criminals are not viable options, the core dilemma is always the same. Is the organization going to pay and decrypt their data, or will they not give in and probably lose their data?

While it is thus possible to reduce all moving parts of a ransomware scenario to this twofold dilemma, to pay or not to pay, this does not make finding the answer any easier. Both options have implications in terms of business continuity, ethical concerns, stakeholder relations, organizational reputation, possible legal liabilities, financial impact, and in extreme cases, even the survival of the company. Furthermore, the answer to this question must be sought in a specific organizational context, which is different for every business or institution. In addition, the decision has to be taken in a crisis environment, meaning that the subjects making the decisions are dealing with imperfect information, uncertainty, and high amounts of stress. In dealing with ransomware scenarios, organizations react differently, some pay, others do not. Some try to react with full transparency and others try to keep the incident out of the media. Some companies focus on internal matters first and then deal with the outside world. Some organizations focus on their employees first. Others see the clients and the organization's reputation as their priority.

1.3 Research aim and strategy

Decision-making in times of crisis has the characteristics of what is often described as a 'black box.'[15] It can be observed that an organization is being hit by a peril like targeted ransomware. Next, it can be observed that the organization takes crisis mitigating measures, and following from that, it can be examined how an organization (in most cases) overcomes the crisis. What is harder to comprehend is how these internal decision-making processes work and how the decisions aimed to mitigate and overcome a crisis are shaped. And while crisis management and broader management literature have shed a fair amount of light on these decision-making mechanisms, the amount of literature that goes into cyber-related or cyber-enabled crisis management remains scarce. Therefore, this research project seeks to contribute to filling this void and use the phenomenon of ransomware targeting organizations as an object of analysis.

The objective of this thesis is to identify how different factors related to a targeted ransomware scenario determine decision-making in crises like these and seeks to unravel what considerations people have when faced with such a scenario. What is more important: the wellbeing of a client's data or the ethical consideration of not paying a criminal? And, if paying a ransom means that weeks of sustained downtime can be averted, is this something to consider? Also, would cybersecurity insurance that covers payment of a ransom change one's decision to pay? It is questions like these that will be analyzed in this thesis. And in order to do this, the following research question is posed:

What considerations determine crisis decision-making in targeted ransomware scenarios, and how do these considerations influence the decision to pay the ransom or not?

The starting point of the research will be a chapter explaining the methodological considerations this study takes. After that, an literature and conceptualization chapter will be provided. This chapter will conceptualize the threat of targeted ransomware and describe how a ransomware scenario can be qualified as an organizational

[15] Edwards and Elwyn, 'Inside the Black Box of Shared Decision Making'.

crisis. Next, the little existing literature regarding organizational decision-making in crisis and uncertainty situations will be discussed, and a theoretical framework will be provided. The framework used is supplied by Luis Ballesteros and Howard Kunreuther and provides an extensive framework to assess organizational decision-making during crisis events.[16] However, this framework is not designed for the specific context of cybersecurity incidents and was, therefore, evaluated and altered where needed. In this process, all the dimensions and subdimensions of the framework were scrutinized and evaluated in the context of targeted ransomware. By combining current knowledge about ransomware based on insights from cybersecurity vendors and news outlets with an established academic framework, an attempt was made to lift the discussion about targeted ransomware from a practitioner's level to an academic level.

This effort also laid the groundwork for the empirical data collection of this research: a digitally distributed survey under information- and cybersecurity professionals with an advising or decision-making role within Dutch private and public organizations. The central assumption in this strategy is that these professionals shape or at least highly impact decision-making regarding digital matters and that analyzing their perceptions of and decisions in a ransomware scenario is therefore worthwhile. By combing current insights about ransomware with an academic understanding of crisis decision-making, it was possible to establish meaningful hypotheses and survey questions regarding the perceptions and considerations that are important during the resolvent of a ransomware crisis. After the distribution of the survey, the data was collected, ordered, and subsequently assessed using the analytical framework. This analysis was subsequently used to come up with a comprehensive answer to the posed research question in the conclusion of this research, where the UM case was also revisited. In the next chapter, the methodological considerations of the study will be explained.

[16] Ballesteros and Kunreuther, 'Organizational Decision Making Under Uncertainty Shocks', 2018.

Methodology

2.1 Introduction

The two primary research methods that are chosen for this study are a literature study into organizational decision-making in times of crisis and a survey distributed under information- and cybersecurity professionals. The literature study aims to provide a conceptual framework regarding organizational decision-making during a crisis. Combining this framework with current knowledge regarding targeted ransomware scenarios did result in the coming to be of hypothetic variables that could impact decision-making during ransomware scenarios. Using these variables, the survey was composed and distributed among cyber- and information security professionals with advising or decision-making roles in Dutch private and public organizations. After the distribution of this survey, the collected data was analyzed using statistical tools in order to structure the results, analyze them, and in this way, provide an answer to the posed research question.

This chapter aims to describe the scope of this research project and show how the different methods chosen for this project helped in finding a satisfying answer to the presented research question. Furthermore, it will be described what considerations played a role when using the research methods that were selected for these projects and what the limitations of the research strategy are.

2.2 Research scope

In terms of geographical scope, this research project primarily focuses on the Netherlands, and the survey was distributed under Dutch respondents. The why in this consideration is quite straightforward. This thesis is written as part of a graduate internship at Fox-IT, a Dutch cybersecurity vendor. While Fox-IT has quite some international clients, the Dutch client base is the biggest, and using these contacts in order to get access to people to disseminate the survey was considered as the most successful strategy. In order to make the survey as accessible as possible for the respondents, the survey questions were asked in Dutch. In terms of timeframe, this project researched a threat that is developing and happening as we speak. At the time of writing, the Maastricht incident is only months past and thus freshly engraved in public memory. This study thus provides an insight into current events and has a future focus in terms of providing recommendations that could positively shape crisis management in future ransomware scenarios and other digital incidents.

2.3 Literature study and conceptualization of variables

The literature study in this thesis has two main goals. First, to provide an overview of the body of knowledge regarding (cyber) crisis management in the organizational context. Second, to provide the theoretical framework that will inform the empirical part of this project. An overview of what considerations typically are of influence during organizational crisis decision-making scenarios would serve as a good starting point for this project. As the phenomenon of targeted ransomware is relatively new, the academic literature around this subject is very limited and on the crisis management side even non-existent. However, in order to still have solid theoretical underpinning to the empirical part of this thesis, an existing organizational crisis decision-making framework, presented by Ballesteros and Kunreuther, was combined with factors that are specific for ransomware scenarios so that it can be used to study our referent object thoroughly. The framework is composed of three different dimensions that study the organization on a different level. For each dimension, different variables are presented that influence decision-making. Examples are stakeholder relations, communication strategies, and financial and business incentives. In the next chapter, the framework will be explained in further detail.

Combining the different dimensions of the framework with the specific context of ransomware attacks will not only make the framework applicable for this kind of crisis but will also serve as a platform for the operationalization of the survey questions. For example, Ballesteros and Kunreuther argue how the institutional context of a specific country of operation can influence the decision-making process regarding the mitigation

of a crisis.[17] Combining this with the fact that the Dutch government has an active policy of persuading organizations to never pay a ransom demand, could lead to a statement in the survey like: "*Because the government advises against paying ransomware actors, I will always advise/decide not to pay the ransom demanded.*", to which respondents can then indicate to what extent they agree or disagree with this. The alteration of the theoretical framework so that it can be used on the specific phenomenon of targeted ransomware thus also serves as a tool for the operationalization of the survey.

2.4 Survey

The core of the empirical investigation of this research is a digitally distributed, self-completion questionnaire. The main goal of this survey is to assess how cybersecurity professionals perceive the threat of targeted ransomware and what their priorities are during such an event. The variables composed in the theoretical framework serve as a mechanism that will help to assess how different considerations influence the decision-making of the respondents during targeted ransomware scenarios. Furthermore, the questionnaire will ask questions going into personal attitudes about the subject. A self-completion questionnaire is chosen because this strategy gives the possibility to question a large pool of experts in a relatively short amount of time.[18] Another important upside of the survey method is that because the survey is anonymous, the respondents can provide insights into the handling of ransomware incidents without the risk the shared information is tracked back to the organizations they work for. This may lead to more openness of the respondents.

The survey has been designed using the Qualtrics survey software, a comprehensive survey tool of which Leiden University owns a license that can be used by its students. In order to ensure anonymity, the software has been configured so that it was not possible for the researcher to get insights into personally identifiable information like IP-addresses. Before the respondents could start the survey, they had to agree to certain terms and conditions about the use of their provided data. This statement can be found in appendix 1.

The survey itself has four different parts. The first part of the survey collects general information about the respondents so that later on when the data is analyzed, comparisons can be made between, for instance, private and public organizations and small and large organizations. The data collected with these questions can also be used to make an assessment in terms of over- or underrepresentation of certain groups in the dataset and about the knowledge level of the surveyed professionals. Furthermore, using the characteristics, an assessment can be made about the respondents being part of the target population or not. If this is not the case, the response will not be included in the final dataset.

The second part of the survey goes into the general attitudes the respondents have about the threat of targeted ransomware. This section features important questions going into the dilemma of paying or not and the ethicality of this dilemma. It is important what basic belief the respondents have about ransomware before the survey goes into detail. The third section of the questionnaire poses specific questions composed by using the theoretical framework and aims to get an in-depth insight into the considerations of the surveyed professionals.

However, this section questions the different factors in separate questions and thus does not provide insight into the different factors of a ransomware crisis in terms of the relative importance towards each other. Therefore, in the fourth and last section of the survey, respondents are provided with a scenario that described that their organization was hit by a ransomware attack and that the lion share of the IT infrastructure became encrypted and that because of this, organizational processes had come to a standstill. With this scenario, nine different factors that could influence the decision to pay or not pay the demanded ransom are provided, and the respondents are asked to indicate to what extent the various elements would be important in their decision to advise or decide to pay the demanded ransom or not. In order to do this, the respondents were asked for each

[17] Ballesteros and Kunreuther, 6.
[18] Bryman, *Social Research Methods*.

factor to move a slider between 0 (not important) and 100 (most important). By calculating the mean score given per factor and ordering them for high to low, an assessment can be made that describes the different factors and 'ranks' them from most important to less important.

2.5 Questions

A complete list of the 46 questions presented to the respondents can be examined in appendix 2; this document includes all questions, a translation into English, and the answering possibilities. It can be observed in the document that most questions have a 'Linkert scale' as the answering option. This scale serves as an objective scale to measure the intensity of feelings about a certain issue, theme, or other research of interest.[19] The questioning method works using the following method: instead of direct questions, respondents are presented with statements also known as 'items,' like, for instance: "*Paying a ransom contributes to the survival of criminal networks and is therefore unethical.*". Respondents are then asked to use the scale to indicate to what extent they agree or disagree with this notion. In this research, the possible answers are 'completely agree', 'agree', 'neither agree nor disagree', 'disagree' and 'completely disagree'. By using a consistent scale of answering possibilities, it is possible to compare the data structurally and objectively. Furthermore, the use of a scale like this has a positive effect on the *internal reliability* of the survey, meaning that scores given by the respondents regarding one concept can be compared with a score given to another concept because the same, objective scale is used.[20] In order to avoid bias, the questions have been formulated as objective as possible and were before publishing presented to research mentors at both Fox-IT and Leiden University to check for this.

2.6 Target population

The targeted respondents for the data collection are information- and cybersecurity professionals with an advising or decision-making role within Dutch private and (semi-)public organizations. The reasoning about targeting this group specifically is that it can be assumed that these individuals are highly involved and/or highly impact decision-making in a cybersecurity incident scenario like a targeted ransomware attack. Furthermore, these individuals have the knowledge and experience to reason about such scenarios in an informed way. By targeting experts, the data collected will serve as a solid foundation to base conclusions on, as the insights derived are not based on the perceptions of just anybody but based on the views and experiences of experts familiar with the topic.

2.7 Sampling strategy

For this research project, it was not possible to adopt a strategy of probability sampling, which is a sampling strategy in where every member of the population has the same chance of being selected for the study because the selection of respondents is random.[21] For a master thesis, it is not possible to spend considerable time and resources towards reaching and convincing hundreds of Dutch cybersecurity professionals to possibly partake in a study and subsequently taking a random sample of respondents to actually collect data from. And because of the novelty of ransomware as an academic object of research, there are no existing datasets that can be used to find an answer to the posed research question. Lastly, even if it was possible to select every cyber- or information security professional in the Netherlands, the chances are high that a large part would not like to share his or hers insights about how they have or would deal with a cybersecurity incident like a ransomware attack, as these are sensitive topics.

In order to still be able to collect data to analyze, a non-probability sampling strategy of voluntary response sampling, also known as volunteer sampling, is adopted.[22] What this means is that the survey is distributed among the population using several digital means like email and social media posts, but the targeted respondents

[19] Bryman, 166.
[20] Bryman, 169.
[21] Bryman, 187.
[22] Jupp, *The SAGE Dictionary of Social Research Methods: Volunteer Sampling*.

have to take it to themselves to choose to participate. The research does thus know where the survey is distributed but does not know who chooses to partake in the study because the study is anonymous. This sampling strategy has two possible pitfalls. First, it could be the case that certain groups who are part of the population are not reached by the distribution, leading to an under-representation of this group in the data. However, by choosing a broad selection of distribution channels, this drawback can be minimized. The second pitfall is more persistent; because the response to the survey is voluntary, it could be so that it is mostly respondents who are very vocal or strong about ransomware that chooses to react to the survey, leading to an overrepresentation of these conceptions and opinions. In order to overcome the stated obstacles, it is thus important to diversify in distribution channels and get as much response as possible. Furthermore, it is important to keep in mind that generalization of the results may be complicated but that because of the novelty of the research area, it seems still worthwhile to conduct the research, as it can later be revisited in larger-scale research projects.

2.8 Distribution

In order to obtain a diverse and large dataset, several distribution channels of the survey were chosen. However, it should be noted that it is unknown how much data was collected using each distribution channel because of the anonymity of the survey.

The primary distribution channels were the Fox-IT social media accounts on LinkedIn and Twitter. Both accounts have around 15,000 followers, who are, presumably, people with some degree of acquaintance with or understanding about cybersecurity and/or information security, and while this does not directly qualify them as fitting respondents, this seems to be the just direction. The LinkedIn post was also shared in numerous private groups going into cybersecurity and related fields of interest.

The second important distribution channel was a cooperation with the Dutch Center for Information Security and Privacy (CIP), a public network organization founded by prominent government agencies that aim to facilitate information and knowledge sharing regarding the field of information security.[23] The organization featured the survey on its internal information-sharing network and invited members to partake in the survey in an email. The cooperation with CIP was useful in reaching respondents active for public organizations because they are the go-to information sharing platform regarding information security in the public sector.

To further diversify the distribution, the questionnaire was also shared on the forum of the Dutch cybersecurity forum and news outlet security.nl, which has a large and vivid community with professionals in the field of information- and cybersecurity.

2.9 Data analysis

After the data was collected, it was subjected to analysis using the statistical tool IBM SPSS 26. The examination of the data serves as the core of this research project. By combing the collected data with the theoretical framework, insight into the preferences, considerations, and priorities of the targeted professionals regarding the handling of a ransomware crisis is provided. The data analysis consists of three parts. The first part of the analysis is to give a general characterization of the data set, describing, for instance, if certain organization types or sectors are over- or underrepresented in the dataset and what this means for the conclusions that can be drawn from the data.

The second part of the data analysis features the general considerations and preferences of the respondents regarding the phenomenon of targeted ransomware. General ideas about payment, ethical concerns of doing so, and the importance of business continuity in the decision-making process will be discussed. Furthermore, this section also features the earlier discussed consideration ranking, listing nine different considerations present in

[23] ‘Home NL - Cip-Overheid’.

a ransomware crisis and their relative importance/priority, according to the questioned experts. This first interpretation of the data serves as the basis for the structural interpretation of the data using the theoretical framework.

The last part of the analysis consists of the combining of the conceptual framework with the data collected. Each dimension and its subdimensions are interpreted using the questions that were operationalized for this specific dimension, and the findings are discussed. In most cases, this is be done by presenting the data visually and interpreting it with the help of the framework. It is important to stress that, in most cases, the goal of doing this is not to establish hard statistical significance using in-depth statistical means. The goal of the analysis is to describe the collected data and provide interpretations through real-world examples and theoretical reasoning, and, in doing so, provide explanations for possible relationships in the data. Because of the novelty of the research area and the relatively small *n* of the dataset finding, statistical significance is thus not the goal, but describing general patterns and providing a meaningful interpretation of these possible relationships is. However, in order to not completely discard the looking for statistical significance, the cross-sectoral comparison of the considerations ranking includes an independent t-test that tests for statistical significance, the ramifications of this will be further discussed in the analysis chapter itself.

2.10 Limitations

Like with every research strategy, the chosen approach towards solving the posed research question has some limitations. In order to minimize the negative effects of these limitations, it is important to be aware of them. A big overarching factor in the limitations of the research is the novelty of cyber crisis management as a research area and cybersecurity as an academic discipline as a whole. In a recent article, Brandon Valeriano points out that current studies into cybersecurity, especially those in the social sciences, miss "*research methodologies and considerations of epistemological outlooks*."[24] Researching a rapidly developing threat like targeted ransomware in a research area that has little to no existing academic foundations is thus easier said than done. Furthermore, it should be noted that the natural context of a master thesis means that there is limited time and manpower available, which means that there will always be some stones left unturned.

One of the biggest limitations of this research project is the small sample size of the dataset, with a sample size of 57 usable responses it is not possible to draw conclusions that are directly generalizable to the real world. This is, therefore, also not the objective of this study. This research project should be seen as an explorative study that lays the foundation for future research into cyber crisis management and the developing threat of targeted ransomware. In doing this, certain relationships will be suggested, and possible explanations for certain data patterns will be provided. However, it is thus important to stress that it could be so that these data patterns are caused by certain biases, misrepresentations, or other errors in the data. The conclusions this research draws should thus always be approached with caution and should not be interpreted as direct reflections of what happens in the real world.

A second limitation of this study is that it draws conclusions on only one primary empirical data source, the data collected using the survey. Ideally, the data from the survey had been combined with other data sources like, for instance, interviews with cybersecurity professionals who had actually fallen the victim of a targeted ransomware attack within their organization. The data from interviews like these could have provided important context to the data described in the analysis. However, time restraint and the context of the COVID-19 pandemic unraveling during the research period made the conducting of such interviews not realistic. While interviews as a primary data source were thus not achieved, it was found that publicly available accounts of ransomware

[24] Valeriano, 'The Failure of Academic Progress in Cybersecurity'.

experiences like Maastricht University's *Lessons Learnt* report and the extensive inquiry provided by the Inspection for Education can also serve as viable sources to provide context to the collected data.[25]

A third limitation of the study is that because the survey questions were operationalized using the provided analytical framework and current insights publicly know about ransomware, it could be the case that certain aspects of the crisis management implications of ransomware were not covered by the survey. It could thus be the case that somehow, a vital aspect of the decision-making process was missed and is not included in the survey. However, the survey features 46 questions and can thus be regarded as extensive, and it is therefore assessed that this last limitation should be regarded as a possibility but not a certainty.

[25] University of Maastricht, 'UM Cyber Attack Symposium – Lessons Learnt'; Ministerie van Onderwijs, 'Rapport Cyberaanval Universiteit Maastricht'.

Literature and Conceptualization

3.1 Introduction

This chapter aims to lay the groundwork for the empirical investigation and analysis of this research project. This means that key concepts regarding targeted ransomware will be defined so that it is clear what is meant when these concepts are used. Furthermore, this chapter seeks to give an overview of the literature regarding crisis management, decision making, and dealing with uncertainty. The concepts derived from this will be formed into a framework for analysis for the empirical research part. Combining this framework with current knowledge about targeted ransomware derived form (limited) academic research, cybersecurity vendors reports, and news outlets results in an a-priori assessment about what variables may be of influence during a ransomware crisis and how they could influence decision-making. These hypothetic variables are subsequently used throughout the empirical part of this research.

3.2 (Targeted) Ransomware

A logical place to start is to provide a detailed explanation of what ransomware entails, what categories exist, and how it proliferates. A simple but fitting definition is provided by Morse and Ramsey: ransomware is a piece of malware on a computer, server, or mobile device that locks or encrypts data with the intent to exchange a ransom payment for a decryption key.[26] The first documented ransomware attack dates back to 1989. The campaign, which was later dubbed the AIDS-trojan affair, was set up by a Harvard evolutionary biologist named Joseph Popp. After being rejected for a World Health Organization job, Popp sought revenge on the academic community researching Aids and HIV, of which he was a prominent member. During a yearly Aids conference in Switzerland, Popp distributed 20 thousand floppy drives, which, according to the label, contained a questionnaire regarding Aids research. However, the floppies were also preloaded with what is called a logic bomb, a piece of malware that would install itself on the PC, wait for it to be turned on and off for 89 times, and on the 90th time encrypt its files and hold the computer ransom. If the victims wished to obtain a decryption key and unlock their files, they were instructed to send $189 to a P.O box in Panama, along with a reference number. Because of this difficult process and the fact that a workaround was quickly found, Popp failed to benefit much from the campaign and was later arrested and tried for extortion.[27]

Over time the modus-operandi of actors employing ransomware has evolved, and ransomware attacks became more and more sophisticated. The first widely distributed strains targeted consumers and held them ransom for relatively low amounts of ransom. These strains would be distributed through large phishing campaigns or pose as legitimate files downloaded from the internet. These campaigns have been active since early 2005 and would be to become the most common form of ransomware for a long time. A famous form of this untargeted consumer ransomware was the ‘police’ ransomware, which would lock a person's computer and show a screen made to look like a law enforcement campaign, targeting online misconduct. The owner of the PC would be accused of all kinds of online misbehavior and face legal consequences unless it would pay an online ‘fine’ to the police.[28] While these campaigns were annoying to consumers affected, the overall impact and effectiveness was quite limited, especially when initiatives like NoMoreRansom.org became more effective in distributing decrypting tools designed for these kinds of strains.

In the last few years, ransomware has become more targeted, more sophisticated, and, most importantly, more destructive. To better understand the contemporary threat landscape regarding ransomware, a categorization by

[26] Morse and Ramsey, ‘Navigating the Perils of Ransomware’.
[27] Waddell, ‘The Computer Virus That Haunted Early AIDS Researchers’.
[28] Palmer, ‘What Is Ransomware?’

SophosLabs is used. This cybersecurity vendor is known as a leading entity on the subject. Their categorization features three distinct categories.[29]

- **The Cryptoworm**: this kind of ransomware behaves like a worm, which means that it propagates by replicating itself onto connected systems in order to get as many infections as possible. The highly disruptive state-sponsored ransomware campaigns in 2017, known as WannaCry and NotPetya, are well-known examples of this kind.

- **Ransomware-as-a-Service (RaaS)**: is sold/rented out on the deep-web to people to those that are deemed trustworthy. The core of this business model is that the people who create and maintain the ransomware are not the ones that (exclusively) employ it against targets. In many cases, but not always, the creators of the ransomware take a percentage of the revenue the attackers make. This kind of ransomware has been spotted in the wild as part of highly targeted campaigns at organizations, but also untargeted mass infection campaigns aimed at consumers. GandCrab and Sodinokibi are well-known examples.

- **Automated Active Adversary:** in this category, highly capable attackers use large phishing campaigns or scan the internet for IT systems from organizations that they can attack, often via exposed and misconfigured RDP (Remote Desktop Protocol) services. When such a system is cracked, it is used to get a foothold inside the target organization's network. From there, they plan their attack carefully, attempt to acquire the highest privileges, and move latterly through the network to spread the malware as far as they can and create maximum damage. A well-known entry point for these kinds of attacks is thus the RDP protocol, which is used by employees to work remotely. However, these protocols can be brute-forced and cracked credentials to these services are often sold on the deep web. SamSam, Ryuk, BitPaymer, and LockerGoga are examples of this kind of ransomware.

In this research, the focus will lay on the last two forms as these categories. This means that individual ransomware victims fall outside the scope of this research. For the sake of clarity, the RaaS and Automated Active Adversary are combined in what is typified as 'targeted ransomware' or 'big game hunting' in this thesis. And while it is true that often attacks on organizations are partially opportunistic rather than fully tailored, as is the case with these attack strategies, they are fundamentally different to the attacks aimed at consumers, which are often described as a 'shot of hail' or a 'fire and forget' campaign that could spread mostly autonomous and could sometimes infect thousands and thousands of computers in a few hours.[30] While targeting an organization may be opportunistic that the term 'targeted' may suggest, it takes time and skill to compromise an enterprise network successfully. Therefore, and because this is the term that is used throughout the cybersecurity community, targeted ransomware seems a fitting term in describing the object of analysis in this research.

3.3 Targeted ransomware as organizational crisis

Crisis decision making in targeted ransomware scenarios is the central theme of this research. But what defines a crisis, and what are the characteristics of a ransomware crisis? An established definition of an organizational crisis is provided by Pearson and Clair: *"An organizational crisis is a low-probability, high-impact event that threatens the viability of the organization and is characterized by ambiguity of cause, effect, and means of resolution, as well as by a belief that decisions must be made swiftly."*.[31] While this definition seems comprehensive, it does not comprehend that crisis often appears as a surprise to decision-makers. One could

[29] Loman, 'How Ransomware Attacks: What Defenders Should Know about the Most Prevalent and Persistent Malware Families'.
[30] Security Boulevard, 'SHARED INTEL: How Ransomware Evolved from Consumer Trickery to Deep Enterprise Hacks'.
[31] Pearson and Clair, 'Reframing Crisis Management'.

argue that this element of surprise is precisely what makes a crisis a crisis, certainly in ransomware scenarios. Another definition provided by Herman does include this dimension; according to this characterization, a crisis has three distinct *conditions: (1) a surprise to decision-makers, (2) a threat to high-priority goals of the organization, and (3) a restricted amount of time available to respond.*[32] Throughout this research, an organizational crisis shall be defined along the conditions provided by Herman.

With these conditions, it can be defined when a ransomware attack qualifies an organizational crisis and what is meant with a successful targeted ransomware scenario. The first condition, *the element of surprise*, is essential in a ransomware scenario. Attackers try their utmost to stay undetected until the files and systems of the victim are encrypted. Logically a ransomware attack cannot be successful if the element of surprise is lost. This would mean that an organization is aware of the fact that someone is in their network to extort them and does not act, a very unlikely scenario. What can be the case, however, is that attackers are noticed but that the measures taken to prevent the attacks of encrypting data are not sufficient. While the total element of surprise will be lost in this case, the attack will still be successful. The second condition, *obstruction of high-priority goals*, seems more important in qualifying an attack as successful. One can imagine that to trigger an organizational crisis, a ransomware attack has to go further than only encrypting a limited number of workstations in the marketing department. To spark an organizational crisis, an attack has to encrypt systems or data *vital* to the *core business* of the organization. What this data or systems are is of course sector and organization specific. The last condition, *limited time to act*, is directly connected to the second condition. If the core business of an organization is in jeopardy because systems are encrypted, the time that is available to get these systems up and running again is limited. For every minute, the organization is not operating properly, the costs rise, and business vitality is threatened.

3.4 Decision-making during organizational crisis

While the body of knowledge around the management of organizational crises is extensive and covers almost all aspects of dealing with organizational crises, this research project has identified that research into the processes and factors of the actual decision-making process during a crisis is still somewhat underdeveloped. While these processes are studied, the conceptualizations around this subject often fail to give comprehensive explanations of what considerations and factors shape decision-making during a crisis. While some studies do try to give insight into decision-making processes, these studies often stay at the psychological level and describe decision making as an interplay between cognitive and intuitive deliberations and fail to provide the organizational context or vice-versa.[33] However, in order to carry out a coherent empirical investigation, building on present theoretical foundations is necessary. Therefore, the insights provided by Ballesteros & Kunreuther in their 2018 working paper *Organizational Decision Making Under Uncertainty Shocks* will be used.

In this work, the researchers provide a comprehensive framework for organizational decision-making during *uncertainty shocks.* These shocks are defined as "*exogenous hazards whose welfare effects spread across industries and markets, such as natural disasters, terrorist attacks, technological disasters, and financial crises."*[34] While a ransomware scenario is not the same as such an extreme event, there are quite some similarities that can be observed when comparing an uncertainty shock with a successful ransomware attack.

[32] Hermann, *International Crises*.
[33] Dionne et al., 'Decision Making in Crisis'; Li, Ashkanasy, and Ahlstrom, 'The Rationality of Emotions'; Pramanik et al., 'Organizational Adaptation in Multi-Stakeholder Crisis Response'; Choi, Sung, and Kim, 'How Do Groups React to Unexpected Threats?'; Kunreuther and Useem, *Mastering Catastrophic Risk*.
[34] Ballesteros and Kunreuther, 1.

Both scenarios can lead to a complete standstill of an organization's core business, impact stakeholder relationships, come as a surprise, and can even seriously threaten the survival of an organization.[35]

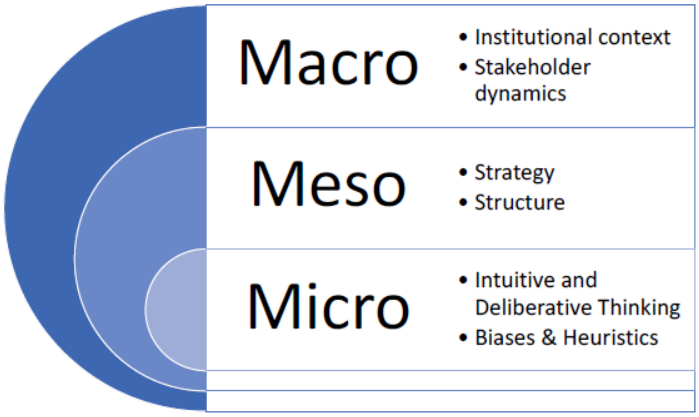
Ballesteros & Kunreuther make the same observation about the gap in the literature regarding organizational decision-making as this study has identified. The authors argue that in dealing with uncertainty and crisis conditions, there is too much emphasis on risk management, an approach which, according to them, fails to grasp the greater complexity of internal and external events in these situations. In order to fill this void, the working paper provides *"a theoretical framework that captures the multidimensional complexity of organizations preparing for, coping with, and recovering from exogenous uncertain disruptions."*[36]

The framework combines insights from cognitive psychology with factors like organizational structure and strategy and subsequently connects these variables with institutional theory going into stakeholder relationships, institutional dynamics, economic incentives, and business continuity.[37] As this framework thus takes a holistic approach towards decision-making under crisis conditions, the framework seems a useful tool that will help to dissect decision-making in targeted ransomware scenarios. The coming paragraphs will discuss the framework and purpose alterations where needed so that the framework can be translated into an empirical research strategy aimed at answering the posed research question.

3.5 The Framework

In their analysis, Ballesteros & Kunreuther identify three dimensions that are of influence in decision-making under conditions of crisis and uncertainty. The first dimension is the *micro* dimension and goes into how managers attend to a phenomenon, perceive it as threats, communicate about this, and act and coordinate with others in order to mitigate these threats. This dimension primarily draws from psychological studies. The second dimension, the *meso* dimension, describes how strategy, defined as goals and initiatives of an organization, combined with the structure, defined as the formal mechanisms of communication and authority of an organization, constitute the collective action taken when dealing with uncertainty and disruption. This dimension thus goes into the organizational context around decision-making. The third dimension, the *macro* dimension, describes how institutional and external contexts, like norms, laws, and for instance, stakeholders' dynamics, influence decision-making in a crisis context.[38]

Figure 1. The three dimensions of organizational decision making under uncertainty shocks



[35] ZDNet, 'Company Shuts down Because of Ransomware, Leaves 300 without Jobs Just before Holidays'.
[36] Ballesteros and Kunreuther, 1.
[37] Ballesteros and Kunreuther, 1.
[38] Ballesteros and Kunreuther, 1–18.

3.6 Micro Dimension

This dimension uses insights from cognitive psychology to describe how individuals make decisions when faced with uncertainty. The foundation of this dimension draws on the well known and Nobel prize-winning research presented by Daniel Kahneman. In his 2011 book 'Thinking, Fast and Slow' Kahneman describes how people, when faced with decision-making under uncertainty, use a combination of two kinds of thinking in order to make decisions. The first kind, intuitive or 'fast' thinking makes up for 98 percent of our thinking and are the rapid and subconscious decisions people take when faced with a problem or emergency. The second way of thinking is the deliberative and 'slow' kind that describes the more rational and long term decisions making humans use to find solutions for difficult problems.[39] When an organization is faced with a serious disruption like a ransomware attack, one can observe both fast and slow thinking being used to resolve the crisis. Intuitive thinking can be seen in IT personnel running around in the building, trying to unplug network cables in order to stop the spreading of the ransomware. Later on, deliberative thinking can be observed when a recovery plan is put together, and executives evaluate the crisis and create plans and procedures in order not to fall victim to such a crisis again.

Using this theory as a foundation and drawing from in-depth interviews conducted with numerous organizational managers, Ballesteros and Kunreuther have identified different behavioral and psychological characteristics in the decision-making of managers faced with uncertainty shocks.[40] They show that managers often have difficulty even imagining that a certain shock could hit their organization. When one can not even imagine that, for instance, a ransomware attack could hit the organization, it is evident that an organization is not properly prepared for such an event. The research also shows that managers are often overconfident in their assessment of a certain risk, also leading to under-preparedness of the organization. Furthermore, managers are often more focused on preserving the status-quo than looking forward to possible threats that could harm the organization. This, combined with a tendency for short-time horizons, often leads to under-preparedness of organizations faced with uncertainty shocks.[41]

Ballesteros and Kunreuther put up a rather negative but nonetheless interesting perspective on the (dis)ability of managers to prepare for events that have a small chance of occurring but a high impact on an organization. While the biases and heuristics presented in their research are well-argued and are indeed based on a solid foundation of empirical evidence, it seems that the identified psychological phenomena that are discovered are not fully elaborated. The authors claim to provide a framework that explains decision-making under crises caused uncertainty shocks. Yet, the different factors presented in the micro dimension like, for instance, overconfidence, misestimation, and the short-time horizons exclusively describe how managers and their organizations fail to prepare for uncertainty shocks. While it may well be that these factors thus influence the *coming to be* of a crisis because of the ill-preparedness of an organization, the presented factors have little to do with actual decision-making *during* a crisis. For this reason, the decision was made to exclude the micro dimension from the empirical and analytical part of this research project. While it would be interesting to research how the psychological phenomena described by Ballesteros and Kunreuther influence the preparedness of organizations for a ransomware attack, this is not the aim of this study. Furthermore, it should be noted that this research project does not aim to provide a psychological study into decision-making, but instead tries to give a broader organizational perspective on the implications of targeted ransomware.

3.7 Meso Dimension

Ballesteros and Kunreuther, drawing from earlier work in organizational behavior, define an organization as *a system of collective action among individuals and teams with different preferences and information that*

[39] Kahneman, *Thinking, Fast and Slow*.
[40] Ballesteros and Kunreuther, 'Organizational Decision Making Under Uncertainty Shocks', 2018, 14 - 17
[41] Ballesteros and Kunreuther,14 - 17

operates under a specific institutional context.[42] When faced with an uncertainty shock like ransomware, the system is disrupted, leading to increased behavioral complexity. In this complex system of actors and structures, organizational literature has overemphasized the role of top-level managers.[43] During an organizational crisis like a ransomware attack, employees on different levels are key in discovering the threat, the communication of crucial information, and working towards continuity and recovery. During the lessons learnt symposium held by Maastricht University, it was stressed numerous times how in the wake of the attack, more than 200 employees worked around the clock to manage the crisis and set up a relief and recovery process.[44] In analyzing how organizations cope with a crisis, one should thus not only look at the boardroom but instead adopt an organization-wide interpretation.

Ballesteros and Kunreuther present the meso dimension to conceive such an interpretation and provide different factors that need attention in order to make this assessment. With the dimension, the authors show how different factors like *strategy*, defined as goals and initiatives of an organization, combined with the *structure*, defined as the mechanisms like economic incentives, communication systems, and authority structures of an organization, constitute the collective action taken when dealing with uncertainty and disruption.[45] While the dimension thus provides a framework for analysis and gives different factors that will be helpful in making an assessment on how different organizational features influence the crisis management implications of a ransomware attack, the dimension as presented by Ballesteros and Kunreuther cannot be directly applied to our empirical interpretation of targeted ransomware. The reason for this is three-fold. First: the framework was designed in order to assess uncertainty events like natural disasters, and while it was already argued earlier why this framework and its concept of uncertainty events are applicable to ransomware scenarios, some alteration is needed. Second: some concepts put forward in the framework are either too broad, to narrow, not applicable to the research, or vaguely described. Lastly, Ballesteros and Kunreuther derive their conclusions and concepts form in-depth interviews and it is not always possible to render these insights directly into concepts that can be tested using a survey. To translate the framework into concepts that can be used in the empirical part of this research, the concepts and insights provided by Ballesteros and Kunreuther will be described and interpreted in connection to targeted ransomware and the posed research question, and, if needed, altered, broadened, narrowed or excluded.

3.7.1 Strategy

The concept of strategy describes how *"the goals and initiatives of the firm shape the biases and heuristics utilized by managers and other employees in their decision-making process."*[46] Ballesteros and Kunreuther show that organizations with long-term future-oriented business-strategy are much more likely to invest in disaster preparation than organizations that are focused on short time profitability. Furthermore, they describe how companies with a flexible organizational strategy, that allows the shifting of resources and adaption of functions were able to handle uncertainty events much better than firms with a rigid organizational strategy.[47]

The observations the authors make about how a long-term focus on survival and flexibility in the organizational strategy has a positive effect on the organization's ability to deal with crisis and uncertainty, seem obvious. This observation also seems to be true in the light of cybersecurity; an organization that has a long term focus on survival is likely to have a lower risk appetite and will probably invest more heavily in security measures than a company that is focused on short term profit. While not empirically tested, the assumption seems evident. What is less clear is what this difference in strategic goals would mean for the handling of a ransomware

[42] Ballesteros and Kunreuther, 'Organizational Decision Making Under Uncertainty Shocks', 2018, 18.
[43] Ballesteros and Kunreuther, 18.
[44] University of Maastricht, 'UM Cyber Attack Symposium – Lessons Learnt'.
[45] Ballesteros and Kunreuther, 'Organizational Decision Making Under Uncertainty Shocks', 2018, 20–24.
[46] Ballesteros and Kunreuther, 18.
[47] Ballesteros and Kunreuther, 19.

incident. Which kind of organization would be more likely to pay, an organization that focusses mainly on profit on the short term, or an organization that also takes long term survival into account?

The research of Ballesteros and Kunreuther only focusses on private companies. As this research project goes into both private and public organizations, this also adds an extra component to the strategy factor. The strategies of public organizations are not definable in terms of short- or long-term profit or survival. It will, therefore, be interesting to see if and how considerations from respondents in private companies differ from those in public organizations as their goals, strategies, and structure are completely different. Another interesting possible division in our respondents could be between those working in what the Dutch National Coordinator for Terrorism and Security (NCTV) has dubbed 'vital processes', and those that are not. Examples of vital processes are payment traffic, internet exchanges, and electrical grid operators. If these processes are disrupted, this could lead to 'severe social destabilization,' according to the NCTV.[48] It will be interesting to see how the crisis management considerations of people working in these processes differ from those who do not.

3.7.2 Structure

The organizational structure is interpreted by Ballesteros and Kunreuther along three different subdimensions; Hierarchy and Authority, Economic Incentives, and Communication Systems. However, it is argued that other factors like the size, the public/private nature, and the sector an organization operates in should also be considered as factors that define an organizational structure, and these characteristics will also be included in the empirical study of this research.

3.7.2.1 *Structure: Hierarchy and Authority*

The organizational structure, defined in the organizational chart, outlines how different employees, teams, and departments set goals, share information, and work together towards the goals of the organization, how this coordinated effort will influence the ability of an organization to deal with disruption.[49] How leadership and authority are shaped inside an organization and how decisions are made thus impact how an organization will deal with disruption. This observation seems plausible; however, empirically testing this notion is not as easy as it seems. The reason for this is that structures of hierarchy and authority are both formed in a formal and informal matter. Unraveling how these structures are formed and play their part inside an organization is something that is not easily examined through an online distributed survey and something that could be done better using in-person interviews. Because of this, the decision was made to give formal and informal structures of hierarchy and authority only limited attention in the analysis.

What is easier to do is ask respondents if their advice and warnings about cybersecurity threats like ransomware are taken seriously. It is often reported that while attacks increase and cybersecurity issues have obtained a much more prominent position in, for instance, the media, it is still difficult to get boardroom decision-makers to actually implement meaningful policy changes and budget allocation to cybersecurity.[50] For this reason, respondents will be asked if they experience this often-heard observation. Furthermore, it will also be assessed if the organizations the respondents work for have implemented emergency and recovery plans for a cybersecurity incident like ransomware because the implementation of measures like these is a good indicator for cybersecurity being on the agenda in the specific organization.

3.7.2.2 *Structure: Economic Incentives*

Arguably one of the most important factors to look at when making an assessment of the impact of uncertainty events and especially when looking at targeted ransomware, is the economic and financial factor. In its core,

[48] Ministerie van Justitie en Veiligheid, 'Vitale infrastructuur - Nationaal Coördinator Terrorismebestrijding en Veiligheid'.
[49] Ballesteros and Kunreuther, 'Organizational Decision Making Under Uncertainty Shocks', 2018, 20.
[50] ZDNet, 'Why Is It so Hard for Us to Pay Attention to Cybersecurity?'; Security Boulevard, 'Despite Increased Attacks, Security Remains Low Priority for Business'.

targeted ransomware is just a profitable business model that uses extortion and disruption to make money. The considerations of at least private companies will probably also be mostly financial, as decision-makers will come up with a cost-benefit analysis what the cost of paying and obtaining a decryption key will be compared with the cost of starting a recovery process without paying the criminals. While considerations like not giving in to criminal enterprises may play a more important role for public organizations than for private ones, one can imagine that also for this kind of organization, the financial implications of the choices that will be made will be reviewed extensively. The decision to pay the ransom demand during the Maastricht University case even resulted in questions in parliament; did Maastricht make the right decision by going with paying? And, was there any public money used to pay off the hostage-takers?[51] The financial component of crisis decision-making during ransomware scenarios is thus a crucial one.

However, the dimension, as explained by Ballesteros and Kunreuther, provides a rather narrow perspective on this important factor. Like in earlier subdimensions, the authors explain how different economic incentives like short-term profit or long-term production security influence the decisions to invest in preparing for shocks. The authors also explain that how managers are rewarded for their work, with, for instance, bonus structures, can influence their decision making.[52] While this approach is interesting, the authors seem to have overlooked the most important factor of the economic side of crisis decision-making: the actual financial impact of an uncertainty event on an organization and the mitigation process connected to such an event. It seems more convincing to explain the economic dimension of crisis decision-making with actual economic factors like projected downtime of business processes, the expected impact on profit, and for instance, the having of insurance that covers disaster recovery. Furthermore, it seems more plausible to assess how factors like these impact decision-making during a crisis than to analyze how the bonus structures of the CISO influence his ideas on how to deal with something like ransomware. Researching if bonus structures have a positive effect on company performance and assessing how structures like these in the past sometimes led to unethical behavior, is an interesting research avenue but falls outside of the research scope of this project.

Therefore in the empirical part of our research, the factor of economic incentives in crisis decision-making is understood as largely financial variables like the amount of ransom demanded, the cost of recovery without decryption in relation to obtaining a key from the criminals, the cost of sustained downtime, the having or not having of cybersecurity insurance that covers ransomware payments and so on. By assessing variables like these, it may be possible to establish how important the economic factor actually is in a ransomware crisis decision-making process.

3.7.2.3 *Structure: Communication Systems*

During a crisis, internal communication is of the utmost importance. Goals need to be formulated, mitigation efforts need to be coordinated, and stakeholders have to be kept in the loop. This is not only a matter of the C-level executives, like the CEO or CISO, communicating their orders to the lower levels to resolve the crisis. For successful crisis management, there has to be open communication in a top-down matter but also in a bottom-up stream.[53] The top-level executive needs to be able to make swift decisions but need information from the ground to make informed decisions, and open communication in both directions is thus of the essence, as Ballesteros and Kunreuther point this out in their framework. It is important to note that during a ransomware attack, email servers can be down, and the internal network could be compromised, and this makes setting up a useful communication stream often a challenge.

[51] Ministerie van Onderwijs, 'Antwoord op Kamervragen over het bericht over cyberaanval Universiteit Maastricht - Kamerstuk - Rijksoverheid.nl'.
[52] Ballesteros and Kunreuther, 'Organizational Decision Making Under Uncertainty Shocks', 2018, 21–22.
[53] Ballesteros and Kunreuther, 23.

Next to the internal communication strategy, there is also an important external dimension of communication during a crisis. However, Ballesteros and Kunreuther seem to forget this important factor. External communication will, therefore, be included in the survey and analysis. It will be interesting to assess if managers favor the road of transparency aimed at openly informing external stakeholders as well as the broader public, or if they will try to keep the incident hidden from the public.

3.8 Marco dimension

In studying the behavior of organizations and the people working for these organizations, it is important to understand that an organization does not operate in a vacuum. The social-cultural and institutional context of the country an organization operates in influences the strategies, goals, and decision-making process of an organization. Furthermore, organizations rarely operate without a vast network of stakeholder and supply-chain relations. The last dimension of the framework provided by Ballesteros and Kunreuther gives insight into this important facet of organizational decision-making during uncertainty events by providing the variables *institutions* and *stakeholders*.

3.8.1 Institutions

In traditional organizational literature, the institutional environment is often regarded as stable. However, in practice, uncertainty events have a tendency to quickly reshape norms, values, and rules that otherwise would change incrementally.[54] While this is especially true for uncertainty events like natural disasters, the financial crisis of 2008, and certainty of the global COVID-19 pandemic that is rattling the world at the moment of writing, this observation is also correct for ransomware. Due to the steep rise of targeted ransomware attacks since 2019, there are, for instance, efforts underway in the US to prohibit the payment of ransomware demands under criminal law.[55] Adding to that, the notorious Russian cybercrime group known as Evil Corp, responsible for the infamous Dridex banking malware and the recent WastedLocker ransomware, has recently been placed on the sanction list of the US treasury department, which means that paying a ransom demand to this actor could be a possible breach of these sanctions, and, therefore, illegal for organizations operating inside and out of the United States.[56] These possible legal implications have gotten a lot of attention in light of the recent ransomware attack targeting GPS service provider Garmin, whose systems and services were offline for more than a week after a WastedLocker attack that demanded a 10 million ransom payment. At the moment of writing, it is clear that Garmin obtained a decryption key, but it is not clear how.[57] It could be that Garmin paid themselves or that a third party broker obtained the key for Garmin. But also more questionable means, like 'hacking back' to obtain the decryption key, are not out of the question, as it has been done earlier.[58]

While there are no plans to make paying ransom illegal in the Netherlands, there is a vivid public debate around the growing problem of targeted ransomware, mainly sparked by the University of Maastricht incident. The Dutch National Police, together with EUROPOL, strongly advises against the payment of the demanded ransom sums trough their collaborative platform NoMoreRansom.org. They argue that by transferring money to the hostage-takers, the victims are keeping the criminal business model alive and that there is no guarantee that the criminals will actually provide decryption keys.[59] Furthermore, the Dutch Minister for Justice and Security urged insurers to stop with cybersecurity insurance that covered the payment of ransomware demands and asked them to focused on prevention instead of mitigation.[60]

---

[54] Ballesteros and Kunreuther, 25.
[55] GCN, 'NY Proposes Outlawing Ransomware Payments'.
[56] Fox-IT, 'WastedLocker'; U.S. Department of the Treasury', 'Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware.
[57] 'Garmin Obtains Decryption Key after Ransomware Attack'.
[58] Hot for Security - Bitdefender, 'Developer Hacks Back Against Ransomware Attackers and Steals...'
[59] Nationale Politie, 'Politie: 'Niet betalen bij ransomware''; 'The No More Ransom Project'.
[60] NRC, 'Grapperhaus wil dat verzekeraars losgeld aan hackers niet vergoeden'.

While there is thus a vivid debate around ransomware in the Netherlands, there is no national government policy that organizations are obliged to follow if they fall victim to a ransomware attack. Other than notifying the Dutch data authority, the *Autoriteit persoonsgegevens* (AP), if there is reason to believe that the hackers have accessed, encrypted or exfiltrated personal data.[61] However, while there is no compulsory policy, the government has an active strategy of advising against payment. It will be interesting to see if this policy has any impact on the considerations of our surveyed IT managers.

3.8.2 Stakeholders

When an organization is faced with an uncertainty event like ransomware, they are often not the only one to suffer the consequences. In the modern integrated economy, organizations are increasingly interdependent, and hardship for one could lead to hardship for the other.[62] When a steel manufacturer in Germany is hit by a successful ransomware attack and they have to halt their production process for two weeks, this can have serious consequences for the supply-chain partners of this company that are dependent on the steel that is produced in Germany. The same goes for customers that are dependent on services that are provided by a company that is hit by a ransomware attack. A growing trend is to attack Managed Service Providers (MSPs), companies that offer services like IT solutions or payroll services to clients, and thus have a high number of clients depending on them. If an attacker manages to compromise the systems of the service provider, it not only harms this company but numerous others, increasing the impact of the attack and, therefore, the incentive to pay.[63]

The fact that often numerous stakeholders are dependent on or impacted by how a ransomware crisis is resolved gives an extra dimension to the decision-making process. Managers have to take into account that their decisions will affect those who are dependent on them. A company can decide not to pay the demanded ransom because aiding a criminal enterprise is not ethical. But what if this decision means that your supply-chain partners or customers lose business or suffer even worse consequences because of the 'ethical' objections of the victim organization? Stakeholder relations could be an important factor in the considerations of managers on how to handle a ransomware crisis and questions regarding this factor are included in the survey.

[61] Autoriteit Persoonsgegevens, 'Datalek door ransomware: wat moet u doen?'
[62] Ballesteros and Kunreuther, 'Organizational Decision Making Under Uncertainty Shocks', 2018, 28.
[63] ZDNet, 'At Least 13 Managed Service Providers Were Used to Push Ransomware This Year'.

Analysis of Results

4.1 Introduction

This chapter will discuss the results of primary empirical research, the online distributed survey, which questions the considerations of cybersecurity professionals regarding ransomware. In the following section, the general characteristics of the collected data will be described. After this, the general considerations of the respondents regarding the threat of targeted ransomware towards an organization will be described and subsequently 'ranked' on the basis of their relative importance. The last subsection of the chapter will analyze the collected data using the structure provided by the theoretical framework that was put forward in the previous chapter.

4.2 The dataset

In the month that the survey was accessible, 62 completed forms were recorded. While there were more surveys started than 62, a large part of them were not completed and, therefore, not included in the dataset. Because five respondents indicated that they did not have an advising or decision-taking role on the subject of information security inside their organization, they were excluded from the dataset, and as a result, responses of 57 information security professionals from the Netherlands were included in the dataset.

As could be expected, when researching a still male-dominated sector like information security, 82.5 percent of the respondents are male. The lion's share of respondents is higher educated, with a least 90 percent of respondents at least having completed a college (HBO) degree or higher. In terms of age, the majority of respondents (86 percent) is clustered between the age 24 and 54, which seems obvious as the target audience consists of people that are working as security professionals and the gross of the working population, in general, is clustered between these age group.

As can be observed in figure 1, there is an over-representation of respondents working within private organizations as compared to public organizations, and only a small fraction of respondents working in semi-public organizations. Because this group is so small and because this type of organization has notable similarities with public institutions in terms of, for instance, the non-profit character, the semi-public organizations will be analyzed together with public organizations. While there is thus an overrepresentation of people working for private companies, the number of respondents working in the vital processes like water supply and the electrical grid, and those who work in 'normal' sectors are evenly distributed, with vital and non-vital both making up around 45 percent of the respondents and with 10 percent saying that they did not know. In terms of size, one can observe in figure 2 that there is an under-representation of small companies (with a maximum of 50 employees) in the dataset and that by far the biggest part of the respondents work for large organizations with at least 250 employees.

Figure 1

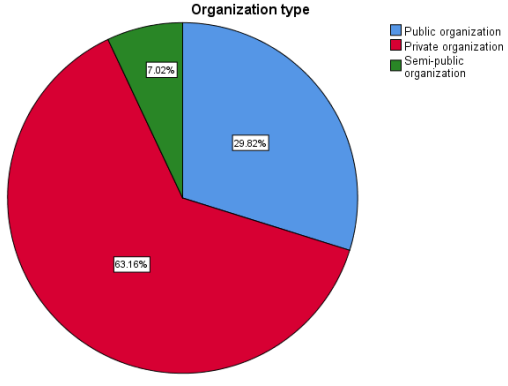
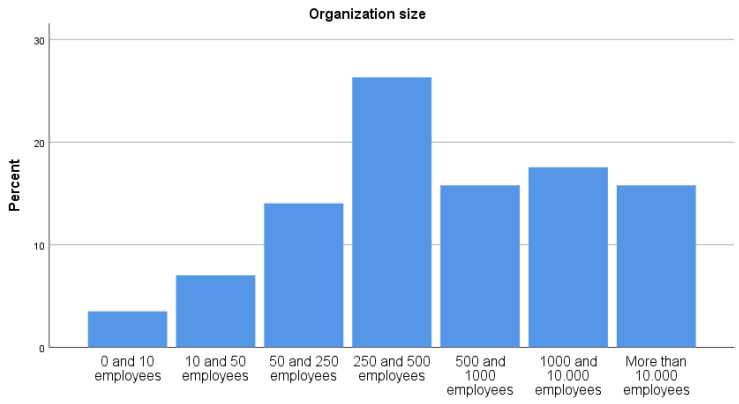


Figure 2



This over-representation in the data can possibly be explained by the fact that the target population consists of information and security professionals and that often smaller companies don't have someone in this exact role or that they outsource information security/cybersecurity to an external party. Furthermore, the dataset also shows that the respondents of the survey actively follow the events around ransomware, with 84.2 percent of respondents agreeing or completely agreeing with the statement: *I actively follow the news around ransomware*. Adding to that, 72 percent of respondents stated that they were technically familiar with the techniques that ransomware actors employ to attack organizations. It can thus be concluded that the dataset represents a group of people that has extensive knowledge of the subject and works in advising or decision-making positions, making them an 'expert group'.

A salient detail that emerges from the data is that almost one-fourth of the respondents said that the organization they work for had previously experienced a ransomware attack targeting their organization. And while a leaked report by the Dutch National Cyber Security Center (NCSC) had already stated that 'dozens' of Dutch companies had been getting hit by ransomware, there are actually only a handful of cases that are known to the public, like the University of Maastricht case and the Wetsus attack.[64] The figures below show that targeted ransomware is indeed not a threat that is missing the Netherlands and that solid academic thinking about the crisis management implications of this threat is ever more important.

Figure 3: Have you previously experienced a ransomware attack within your organization?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes, payment was made	2	3.5	3.5	3.5
	Yes, no payment was made	12	21.1	21.1	24.6
	No	39	68.4	68.4	93.0
	I prefer not to say	4	7.0	7.0	100.0
	Total	57	100.0	100.0	

4.3 General considerations about ransomware

As a starting point of the assessment of the collected data, it is useful to get some insights into the general considerations and conceptions of our questioned respondents. These broad beliefs and opinions regarding the phenomenon of targeted ransomware and the implications of this threat will lay the groundwork for the more in-depth analysis of the data later in this chapter.

Figure 4: If I personally fell victim to a ransomware attack, I would under no circumstances pay the ransom demanded.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Completely agree	24	42.1	42.1	42.1
	Agree	13	22.8	22.8	64.9
	Neither agree nor disagree	11	19.3	19.3	84.2
	Disagree	3	5.3	5.3	89.5
	Completely disagree	6	10.5	10.5	100.0
	Total	57	100.0	100.0	

As a starting point, respondents were questioned about how they would react to a ransomware attack in their personal life, when, for instance, a personal laptop or phone would be encrypted with ransomware, and would they pay or not? Figure 4 shows that a strong majority of respondents agreed or completely agreed with the

[64] 'NCSC: "Tientallen Nederlandse bedrijven getroffen door ransomware"'; 'Openheid beste verdediging tegen ransomeware-aanval'.

statement stating that if they would fall the victim of a ransomware attack, they would under no circumstances pay the ransom demanded. However, there is also a relatively large group undecided on this mater. With only around 15 percent disagreeing or completely disagreeing with the posed statement, it can be assumed that in a personal ransomware scenario, most respondents are not very likely to give in to the ransom demand of a ransomware actor.

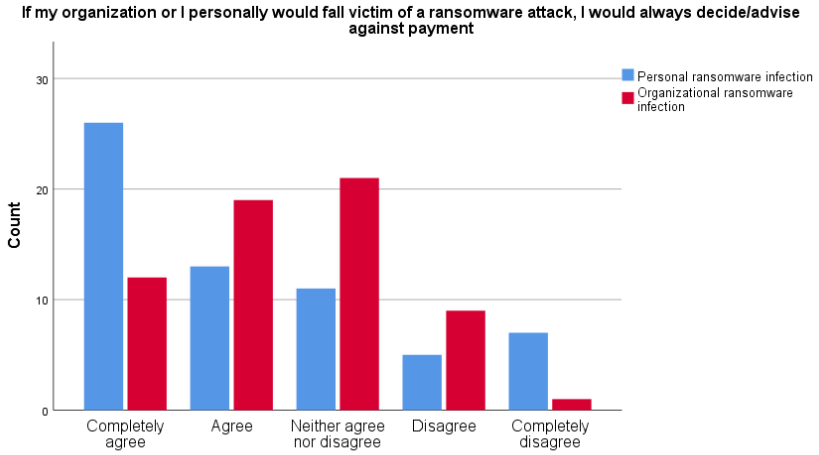
When respondents were asked the same question, but now in regard to their decision or advice when the organization they work for would become the victim of a ransomware attack, the respondents are less explicit in their considerations that with a personal attack. Figure 5 shows that there is still a small majority (50.9%) that agrees or completely agrees with the statement that they would always decide or advise against paying the demanded ransomware, the biggest subgroup is now actually undecided on the mater.

Figure 5: If the organization I work for would fall victim to a ransomware attack, I would always decide/advise against paying the ransom demanded.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Completely agree	11	19.3	19.3	19.3
	Agree	18	31.6	31.6	50.9
	Neither agree nor disagree	20	35.1	35.1	86.0
	Disagree	7	12.3	12.3	98.2
	Completely disagree	1	1.8	1.8	100.0
	Total	57	100.0	100.0	

If figures 4 and 5 are combined into a bar chart, which is done in figure 6, the visualization paints the picture more clearly, and it can be observed that the responses to the question are more centered in the middle of the Linkert scale, with a small majority being undecided on the matter. However, the group that disagrees with the statement is still a small minority of around 15 percent, and this percentage corresponds with the answers given to the question regarding the personal ransomware infection question. Therefore, it cannot be concluded that the respondents are more likely to pay in an organizational ransomware scenario than when they are hit personally. However, what can be said is that the decision to pay or not in an organizational ransomware scenario seems harder to grasp for the respondents than taking this decision in a personal capacity. This conclusion seems logical; the complex organizational context of decision-making during an uncertainty event like a ransomware attack was described extensively in earlier chapters of this research.

Figure 6

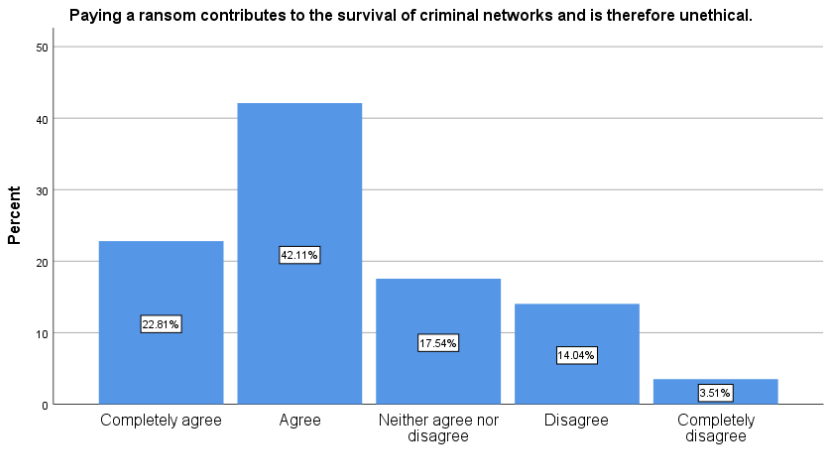


While the distribution of the respondent's answers regarding the dilemma of paying or not paying differs for a personal or an organizational situation, the data shows that generally speaking, the majority of respondents feel

that they are unlikely to pay for a decryption solution to resolve a ransomware crisis. While the exact reasons for this are probably different for every individual respondent, there are some leading arguments against paying, which are often echoed in the debate regarding the problem of targeted ransomware. These arguments have been extensively covered in earlier chapters and were, therefore, also a part of the survey.

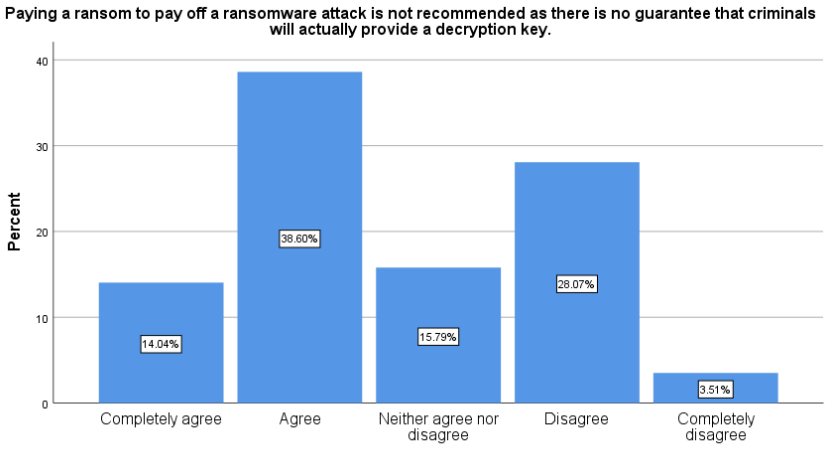
One of the most heard arguments against paying of ransomware actors is the fact that in doing this, you and your organization are actively aiding and abetting a criminal business model, and this should be regarded as unethical behavior. When presented with this statement, visually displayed in figure 7, respondents largely agreed with the notion that paying ransomware actors can be classified as unethical behavior.

Figure 7



Another often-heard argument against paying is the idea that paying for a decryption solution does not guarantee that such a solution will actually be provided. There is no guarantee that the criminals after the payment of the ransom demand will provide the victim with a decryption solution that will work. While this argument is often put up by people and organizations who advise against payment, there is little evidence that this claim is true for targeted ransomware scenarios. As pointed out earlier, ransomware operators are dependent on their reputation of indeed providing a decryption solution for their business model to work. If the reputation of the group behind CLOP ransomware had been bad because in earlier cases the hostage-takers had not provided a decryption solution after payment, the University of Maastricht probably would not have gone through with paying the demanded ransom. As figure 8 shows, the respondents are divided on this subject, with the biggest group agreeing with the statement but the second-biggest group disagreeing with the statement.

Figure 8

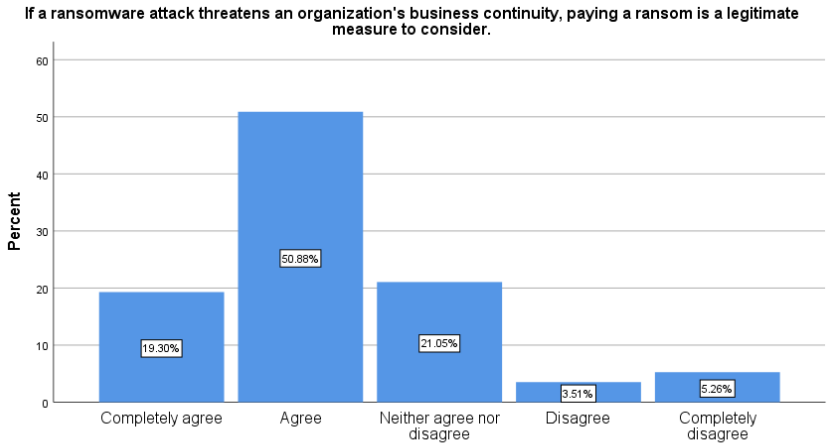


The data described above indicates that the majority of respondents, when asked directly and without further context about the making of a payment to resolve a ransomware scenario, largely declare that they are unlikely to pay for a decryption solution. They also largely agree that paying for decryption contributes to the survival of the criminal business model of targeted ransomware and that paying of hostage-takers should thus be regarded as unethical. While these considerations seem obvious, nobody wants to be extorted and help keep a criminal business model alive, it is important to see if considerations of respondents change, when provided with additional context.

The ethical considerations, as well as the uncertainty regarding the trustworthiness of the criminal actor taking the victim hostage, are both often heard arguments against paying ransomware demand. However, on the other side of the coin, there are numerous reasons that speak in favor of paying the demanded amount. An umbrella-concept in this matter is the notion of business continuity, which *"refers to the ability of a business to maintain continuous operations in the face of disaster."*[65] It is clear that a successful ransomware attack severely limits an organization's capability to maintain normal operations, as most modern organizations are highly dependent on their IT systems.

When asked if the respondents felt that ransom payment would be a legitimate measure to consider if a ransomware attack threatens the business continuity of an organization, the respondents largely approved, with more than 70 percent agreeing or completely agreeing with the statement posed in figure 9. It is interesting to see that the notion of business continuity largely shifted the appetite of the respondents to consider paying for a decryption solution, even though more than half of respondents stated earlier that they would always advise against paying hostage-takers and 65 percent of respondents regard paying a ransom demand as unethical. While the data does not directly imply that when business continuity is threatened, respondents automatically are in favor of payment, the question clearly states 'to consider' as part of the question. However, what the data does suggests, is that while most respondents are not in favor of paying a ransom demand, there may be circumstances that could still have them consider going with paying.

Figure 9



4.4 Ranking the considerations

As described extensively throughout this research, numerous considerations play their part during the crisis management of a ransomware scenario. However, not every factor carries the same weight in the decision-making process of an organization. In order to assess the factors described in the theoretical chapter of this research, an idea needs to be established how the respondents of the survey would 'rank' different considerations and circumstances that could play a part in their decision-making process during a ransomware crisis. This

[65] Rittinghouse, *Business Continuity and Disaster Recovery for Infosec Managers*.

ranking provides a general idea about how the preferences and priorities of respondents are ordered during the handling of a ransomware crisis. This general overview of preferences will help to provide a better assessment of the different theoretical factors put forward in the analytical framework.

In order to measure this ranking of priorities, respondents were provided with a scenario that described that their organization was hit by a ransomware attack and that the lion share of the IT infrastructure was encrypted and that because of this, organizational processes had come to a standstill. With this scenario, nine different factors that could influence the decision to pay or not pay the demanded ransom were provided, and the respondents were asked to indicate to what extent the various elements would be important in their decision to advise or decide to pay the demanded ransom or not. In order to do this, the respondents were asked for each factor to move a slider between 0 (not important) and 100 (most important). Using the data collected by this model, an assessment has been made that describes the different factors and 'ranks' them from most important to less important. The ranking is based on the calculated mean of all responses for each factor. It is important to note that because the ranking is calculated by the mean response of all respondents, there could be big differences in the individual ranking of preferences of respondents. This overview should thus be seen as a general interpretation of the data. Throughout the later stages of the analysis, an assessment will be made to see if individual characteristics or preferences of respondents lead to a change in the general ranking described in figure 10.

Figure 10: Ranking the considerations

	Mean score
Prevent losing crucial data	**87.12**
Preventing long-term stoppages of business processes	**84.93**
The interests of customers and supply-chain partners	**78.47**
Taking reputational damage	**66.16**
Not wanting to contribute to a criminal revenue model	**59.89**
The uncertainty whether the payment actually leads to decryption	**55.21**
The cost of an independently performed repair operation in relation to paying a ransom	**45.00**
The amount of demanded ransom	**41.12**
The advice from the police to never pay a ransom	**34.80**

The highest-ranked priority, preventing the loss of crucial data, seems to be in an obvious first place. At the end of the day, ransomware is about encrypting data, and making an effort to prevent the permanent loss of data crucial to the organization is a convincing priority. Moreover, it should be emphasized that this is a valid concern; the threat actors targeting organizations are highly skilled and are often able to encrypt backup systems as well.[66] The same goes for preventing long-term stoppages of business processes. The interests of customers and chain partners are also high on the priority list of our surveyed population, and this is no surprise; the possible negative effects on customers and supply-chain partners as a result of a ransomware attack has been covered in this research. From the data described above, it can be confidently concluded that the prevention of data loss, business continuity, and the interests of stakeholders are highest on the priority list of the surveyed

[66] ZDNet, 'Ransomware Victims Thought Their Backups Were Safe. They Were Wrong'.

information security professionals. This conclusion is somewhat an open door, but the data reflects this conclusion clearly and is therefore not to be marginalized.

Looking further down, it can be observed that taking reputational damage, not wanting to contribute to a criminal business model, and the uncertainty about actual decryption are the three considerations that are ranked in the middle of the model. It can be assumed that these considerations take part in the decision-making process of our respondents but that they are subordinate to the three main priorities of securing data, business continuity, and stakeholder interests. How these factors are precisely placed in the decision-making process cannot be determined from this model. However, these factors will be covered more extensively with the help of the theoretical framework.

Looking at the three elements that have been placed on the bottom of the model, two general observations can be made. First, the considerations of the respondents do not seem to be particularly influenced by the actual amount of ransom demanded or the cost of such payment in relation to the cost of independently performed reparation operation. This is a somewhat unexpected finding; one would expect that the amount of ransom demanded would have a considerable influence on the decision to pay or not and that a relatively low ransom demand would make payment more likely and vice-versa. A more in-depth interpretation of this result will be provided in the analysis of the economic factor, which is part of the meso dimension of the theoretical framework. The second and interesting observation is that the advice to never pay a ransomware demand put out by the Dutch police does not seem to be an important consideration of our respondents. The institutional pressure that aims to discourage organizations not to pay that was explained earlier seems not to be very effective.

4.5 Structural interpretation of results with the theoretical framework

The coming part of this chapter will combine the collected data with our earlier described analytical framework provided by Ballesteros and Kunreuther. As pointed out earlier, this analysis will focus on the meso and macro dimensions and their associated subcategories. Throughout the analysis, the focus will lay on specific survey questions that were operationalized for the specific subcategory, but the general ranking of considerations described earlier will also serve as a tool to provide a deeper understanding of the subcategories and their relevance during a ransomware crisis.

4.6 Meso dimension

The meso dimension assesses the decision-making process during uncertainty events at the organizational level. The first subdimension of the dimension is the Strategy factor, which describes how short- and long-term strategies of an organization define crisis decision-making during uncertainty events. The second subdimension is the Structure category, which describes how formal and informal structures present in an organization define decision-making during a crisis. The subdimension is divided into three different subcategories, these being: Hierarchy and Authority, Economic Incentives, and Communication Systems. It was also argued that general characteristics like size, the public/private, and vital/non-vital nature of an organization also influence the structure and strategies of organizations; these factors will thus also be discussed throughout the different dimensions.

4.6.1 Strategy

In the theoretical chapter of this research, it was described how Ballesteros and Kunreuther understand the first factor of the meso dimension, the strategy factor, as a factor that describes how the long or short term goals of an organization influence its preparedness for crisis and the decision-making process during uncertainty events. Ballesteros and Kunreuther argue that organizations with clear long-time strategies aimed at survival are much more likely to invest in defenses and preparedness for uncertainty events than organizations that prioritize short

time profit.[67] Following this reasoning, it could be argued that this would mean that when hit with ransomware, organizations with long-term goals or vision would make different decisions than organizations that have more short-term profit-seeking goals. In order to test this hypothesis, a question regarding the organization's long-term goals in relation to short-time profit-seeking was included in the survey. The recorded responses to this question are described in figure 11.

Figure 11: In the organization I work for, long-term survival and service availability is more important than making a profit in the short term.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Completely agree	17	29.8	29.8	29.8
	Agree	21	36.8	36.8	66.7
	Neither agree nor disagree	11	19.3	19.3	86.0
	Disagree	7	12.3	12.3	98.2
	Completely disagree	1	1.8	1.8	100.0
	Total	57	100.0	100.0	

The data shows only a small fraction of the respondents disagree or completely disagree with the statement, saying that short-term profit is more important than long-term survival and availability. When the rest of these disagreeing answers given by the respondents were analyzed further, the data shows that only four of these respondents are actually active for a private organization, two for a semi-public organization, and two for a public organization. As the making of short-term profit can hardly be an objective in a (semi-)public organization, especially compared with something like service availability, it seems that the respondents that choose these options perhaps misunderstood the question. With there being only four respondents in the dataset who work for a private organization able to make a profit and also prioritize this profit over long-term goals and service availability, it seems not worthwhile to provide an in-depth analysis of how the considerations of these individuals differ from the rest of the population. And while it is true that this research bases its conclusions on a relatively small dataset, and this is not necessarily a problem, it seems not sensible to base conclusions on answers provided by only four respondents.

As was pointed out in the theoretical framework, the strategy factor of the meso dimension should be understood in a broader sense than only the notion of long or short-term goals and profit. Strategies adopted by organizations differ per sector, business model, organizational culture, and so on. One could even argue that every organization has a different strategy and that dividing cases in a meaningful matter, only on the basis of something so broad as an organizational strategy, is easier said than done. However, as argued earlier, the public/private divide in organizations does serve as a meaningful and easy to grasp distinction between different organizations. The goals, strategies, and structure of public organizations are radically different compared to private companies, and therefore it seems worthwhile to investigate if the considerations of the respondents are different across this divide.

Besides the public and private divide in the Dutch organizational landscape, it was also pointed out earlier that there is a notable difference in organizations that are in the so-called vital processes and those who are not. Vital processes are operations that are essential for the proper functioning of Dutch society, and the disruption of these processes could be regarded as a threat to national security. Examples of these processes are critical infrastructure like electricity and water-supply companies but also internet exchanges, the police, and the stock exchange.[68] It seems like a logical assumption that these kinds of organizations feel strongly about security and

[67] Ballesteros and Kunreuther, 'Organizational Decision Making Under Uncertainty Shocks', 2018, 18.
[68] Ministerie van Justitie en Veiligheid, 'Vitale infrastructuur - Nationaal Coördinator Terrorismebestrijding en Veiligheid'.

would regard the availability of their services as one of their highest priorities. As the stakes are high with these organizations, it seems worthwhile to explore if the considerations regarding ransomware are different for respondents working in a vital process as compared to those who do not.

In order to measure if there are notable differences between the consideration 'rankings' across the different sectors, the same analysis as in the previous subsection was preformed, but now with cases divided across the different sectors. The results of this analysis are displayed in figure 12. Generally speaking, the data shows little to no fluctuation in the ranking itself; the overall order of priorities is practically the same for the public and private sector and across the vital/non-vital divide. The only exception for this is that public and vital organizations rank the advice from the police to never pay ransom second-last instead of last, switching this consideration with the amount of the ransom demanded. However, the percental difference between these two considerations in the public sector is only 0.1 percent, and should, therefore, not be regarded as substantial. Generally looking at the results of the analysis, it can be assessed that the numerical ranking of considerations of our surveyed professionals is the same across the sectors and that there are no notable differences that can be regarded as significant, except for the small switch of places of the two least important considerations in the vital sector.

The general order of considerations and priorities is thus the same across the different sectors. However, this does not mean that it is impossible to derive some interesting insights from the model displayed in figure 12. In order to do this, attention has to be paid to the percental differences of the mean score given to a particular consideration in a particular sector compared to its counterpart; there can only be valid comparison between the private or public organizations and vital or non-vital organizations. This is because organizations can both be private and vital, public and non-vital, and so on. Because of the relatively small *n* of the dataset, it seems not feasible or worthwhile to produce a comparison between all these subgroups.

Figure 12: Considerations mean scores per sector

	Population (*n* 57)	Private (*n* 36)	Public (*n* 21)	Vital (*n* 26)	Non-vital (*n* 25)
Prevent losing crucial data	87.12	88.14	85.38	83.65	90.12
Preventing long-term stoppages of business processes	84.93	86.25	82.67	81.23	88.92
The interests of customers and chain partners	78.47	79.30	77.04	77.77	78.48
Taking reputational damage	66.16	65.58	67.14	61.65	68.96
Not wanting to contribute to a criminal revenue model	59.89	59.02	62.57	57.84	58.88
The uncertainty whether the payment actually leads to decryption	55.21	50.92	61.38	54.00	55.80
The cost of an independently performed repair operation in relation to paying a ransom	45.00	44.08	46.57	43.88	44.88
The amount of demanded ransom	41.12	40.58	42.04	32.58	46.88
The advice from the police to never pay a ransom	34.80	30.50	42.14	38.69	32.16

In figure 12, the notable fluctuations in the mean score given are highlighted by the rectangles. The threshold for qualification as a notable fluctuation is a difference of at least 5 percent or more in between the public/private

or vital/non-vital divide. Some fluctuations seem logical, and others seem counterintuitive, for example, it seems logical that the advice from the police to never pay a ransom demand would find more fertile ground within public organizations that within private organizations, as the police are part of the public sphere and its advice would likely be adhered to sooner in this setting than to within private organizations. A 12 percent variation in importance score thus seems like a logical result. The same goes for the consideration concerning the idea that payment does not necessarily lead to decryption, a suggestion that is often echoed by Dutch government institutions like the NSCS.[69] Although it was pointed out earlier that this observation is not completely accurate in relation to targeted ransomware aimed at organizations, it seems logical to assume that this idea is more widely believed among public organizations than within private companies and that the fluctuation in the score could possibly be attributed to this. The figure also shows fluctuations that seem more counterintuitive and are not as easily explained as the two fluctuations in the public sector. It seems that respondents from the non-vital sector gave a notable higher mean score to the two highest-rated considerations regarding data loss and business stoppages. This is an unexpected finding; one would think that organizations that are regarded as vital processes, meaning that their disruption could lead to 'severe social disruption,' would have considerations connected to business continuity as their utmost priority. And while the sector does rank these continuity factors the highest in a relative sense, the numerical fluctuation with its non-vital counterpart does catch the eye and makes up for a curious difference.

4.6.1.1 *Statistical significance*

While the sectoral division presented in figure 12 does account for interesting differences in the considerations scores across sectors, it is important to assess if these differences do actually account for statistically significant differences. In order to test for significance when comparing means of a dependent variable like, for example, the factor regarding the advice of the police, against an independent variable like sector, an independent t-test can be used. If the compared means pass the t-test, it can be established that the fluctuation between the two compared means is statistically significant, and it can be excluded that this difference is caused by chance or other irregularities in the data.[70] The complete output of the t-test conducted using IBM SPSS, and a further explanation of the statistical technicalities and procedures of this test can be examined in appendix 3.

The result, however, is quite clear; the only notable fluctuation of the mean score passing the requirements of the t-test conducted is the variation of preventing long-term business stoppages compared between the vital and the non-vital sector. For this reason, this fluctuation is marked with a blue box instead of a red one in figure 12. This outcome is a somewhat surprising and unsatisfying result, as the fluctuation that seems the most counterintuitive is the one variation that establishes statistical significance. However, not being able to establish statistical significance for the found fluctuations using the collected data does not mean that the variations found should be discarded altogether, it just means that it cannot be excluded that chance or other regularities are causing the found fluctuations. However, this goes both ways; finding statistical significance for a variation does not mean that a generalization can be made and that this observation is necessarily true in the real world. What it does show is that there are interesting and surprising fluctuations in the data and that more extensive and larger *n* research is needed to establish if these differences are indeed present in the real world and not only in the dataset used for this research.

4.6.2.1 Structure: Hierarchy and Authority

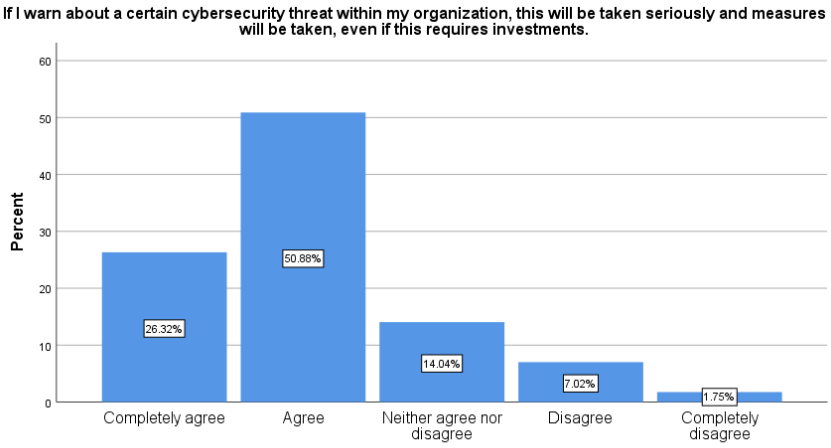
How structures of hierarchy and authority are shaped within an organization influences how capable these organizations are in dealing with uncertainty events. However, as was pointed out earlier, it is difficult to unravel formal as well as informal structures of hierarchy and authority inside an organizational system using an online

[69] 'Cybersecuritybeeld Nederland (CSBN) 2020', 34.
[70] 'Data Analysis - Independent Samples t-Test'; Kenton, 'Why Statistical Significance Matters'.

distributed survey. If one truly wants to dissect such social norms and rules, an in-dept and face to face interview would be a more suitable data collection method. However, in order to not skip this dimension, respondents were asked to what extent cybersecurity issues, and the warnings they provide about these issues, are taken seriously within their organizations. As one can imagine, good preparation for a crisis that might occur one day is essential, and to achieve this, subject experts have to be taken seriously, and their advice needs to be translated into action. Therefore, it was also surveyed to what extent policies like crisis management procedures are actually put in place to deal with the possible implications of a cyber incident like a ransomware attack.

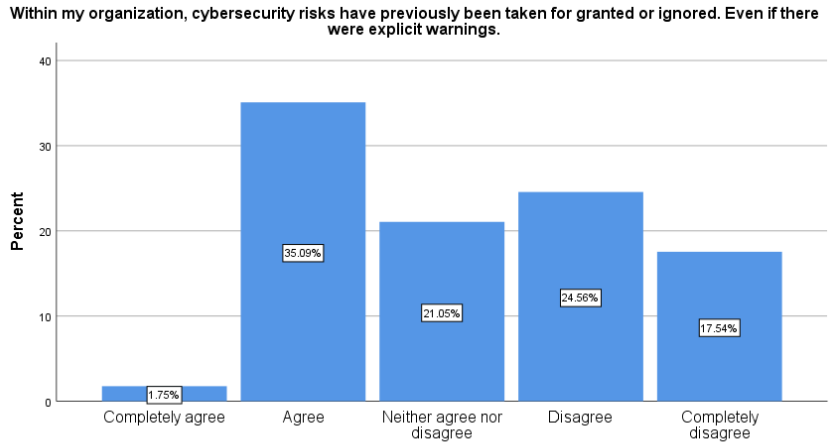
Looking at figure 13, it can be observed that more than 75 percent of the respondents feel that if they warn about a certain cybersecurity threat facing the organization they work for, action will be taken, and investment will be made if this needed. It is reassuring to see that Dutch organizations are indeed listening to their hired information security professionals and do not ignore their advice. However, this answer is not surprising; it would be somewhat odd to hire personnel to an 'advising or decisions-making role in information security' and subsequently not follow up on the advice they give. Adding to that, and as pointed out earlier, the dataset that is used for this research project has an overrepresentation of respondents working in organizations with 250+ employees, and these organizations are more likely to allocate money and manpower for information- and cybersecurity.

Figure 13:



While the questioned professionals generally point out that they feel like their advice is taken seriously, a big group of respondents also points out that in earlier instances, cybersecurity risks have been taken for granted and ignored, even though there were explicit warnings about the dangers of doing so. This data can be interpreted in multiple ways.

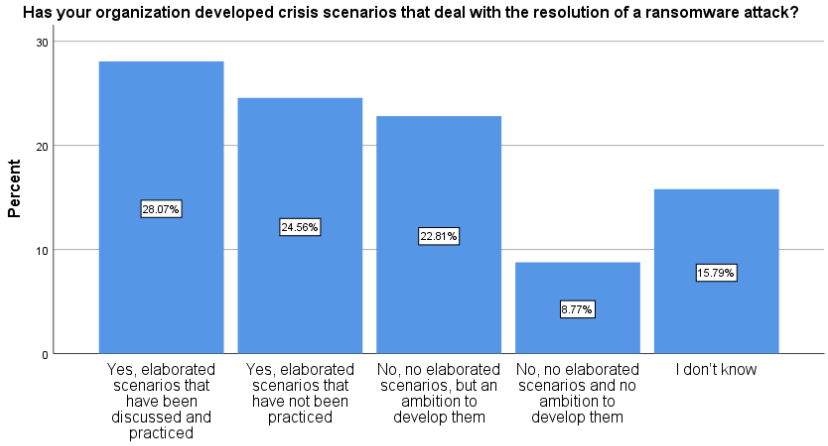
Figure 14:



It could be the case that respondents feel that historically cybersecurity risks would have been underestimated within their organizations, but the raising of awareness in the last decade has led to cybersecurity issues being higher on the agenda of decision-makers and the issue being taken more seriously nowadays. It could also mean that while the respondents feel like taken seriously and their advice mostly adhered to, there are still issues that are ignored and not given the attention that the respondents deem necessary.

Another observation that can be made is that there are notable differences between the maturity level of cybersecurity policies between different organizations. When respondents were asked about the having of crisis management procedures to deal with a high-level cybersecurity crisis like a ransomware attack, the biggest group responded that their organization has indeed implemented crisis management scenarios to deal with such a crisis and that these procedures had also been practiced. However, there is also a big group that does not have procedures in place for such an event, and 1/3 of this group also does not have the ambition to develop this. Furthermore, more than 15 percent of respondents do not know if their organization has developed crisis management procedures for such an event, a number that seems high, especially for a population that would be some kind of expert on matters like these.

Figure 15



Generally speaking and understanding the subdimension Hierarchy and Authority in terms of to what extent our surveyed professionals feel that their concerns are taken seriously and translated into action, multiple conclusions can be made. First, most of our respondents feel like their work taken seriously and translated into action where needed. However, respondents also feel that in earlier instances, explicit cybersecurity risks were taken for granted or ignored. This could be expected; cybersecurity has not always been as high on the agenda is it is today. However, looking at the large group of organizations that do not have contingency plans for an event like ransomware hitting their organization, there is still progress to be made.

4.6.2.2 Structure: Economic Incentives

In the conceptual chapter of this research, it was argued that the economic and financial component of targeted ransomware scenarios could well be the core of the decision-making process when dealing with ransomware. It was pointed out that at least for private organizations - whose key motive it is to make profit - it could be the case that a ransomware scenario could be approached as a purely economic problem, which could be resolved by making a simple cost-benefit analysis. By projecting the cost of an independently performed recovery operation and comparing this to the option of paying in order to obtain a decryption key from the hostage-takers, decision-makers could estimate which option would be the most financially favorable and go with this option. However, the findings in the general considerations ranking did already erode this claim, with the cost of an independently performed repair operation in relation to the amount of the ransom demand ranking third to last and the amount of the actual ransom demand ranking second to last. What the ranking suggests is that decision-making during a ransomware crisis is not merely based on simple cost-benefit analysis looking at costs.

Throughout this subsection, the economic and financial considerations will be compared between public and private organizations

This claim is reinforced with the data presented in figure 16, which shows that for both private and public organizations, only a relatively small minority of respondents agree with the notion that if payment of ransom is the cheaper option, they would decide to go with this. However, this seems not to be the case, both sectors generally disagree with the statement, but the public professionals do feel more strongly about this.

Figure 16

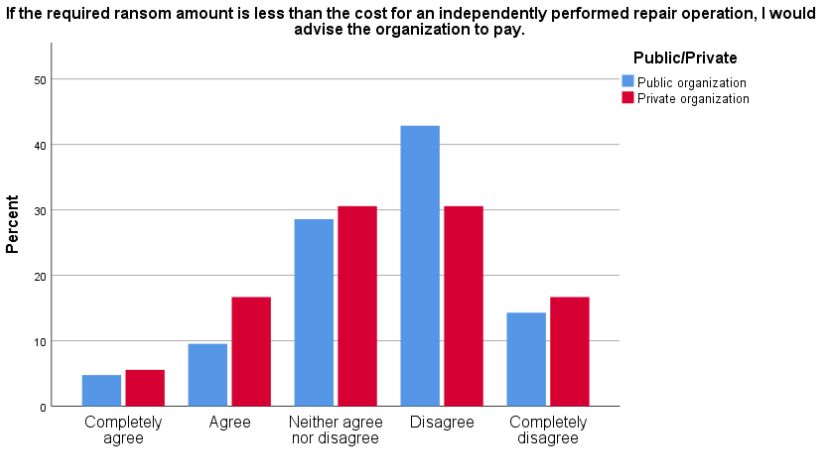
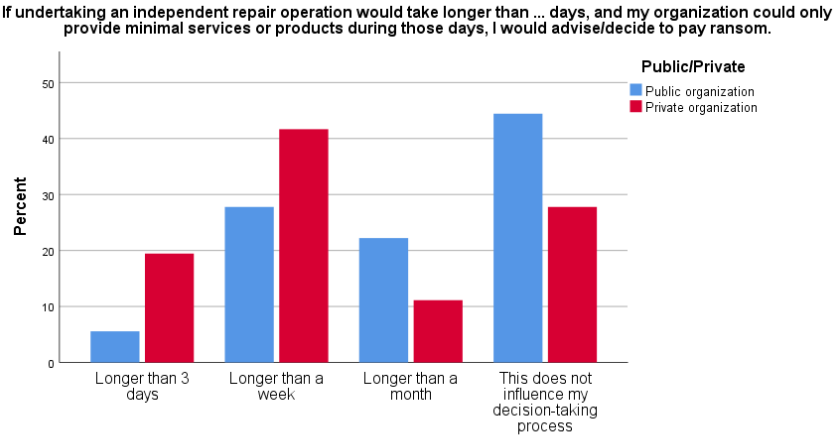


Figure 16 shows that the plain cost-benefit analysis of paying in relation to not paying does not persuade the respondents to consider making payment of a demanded ransom. However, it could be the case that the level of abstraction of comparing the costs of paying or not paying leads to respondents leaning towards not paying. Framing the question in terms of business continuity and downtime instead of the direct cost may lead to a different answer. While the framing is different, business continuity is an economic variable pur sang, as every day that an organization is not able to operate will cost money, both in the public sector and the private sector. In an earlier subsection of this chapter, it was already shown that respondents largely agreed with the notion that when business continuity is threatened, paying a ransom is a legitimate option to *consider*, however, it will now be tested if the factor of projected downtime serves as an incentive for the respondents to decide/advise their organizations to pay.

In order to test this premise, respondents were presented with a question that connects the projected days of downtime when going with an independent repair operation to the incentive to pay. The respondents could choose from a range from one day to more than a month, or answer that projected downtime did not influence their decision-making process. Because of the many options available, the data collected from this question was widely dispersed, so in order to come up with a meaningful assessment of downtime connected to the payment the datapoints were grouped into four clusters: respondents that would advise or decide to pay after three days of downtime, after a week of downtime, after a month of downtime and those who argued that this notion does not influence their decision-making process. In order to compare this consideration between groups, it was also decided to provide a comparison between public and private organizations. As argued earlier economic incentives are arguably the most distinct between those two groups; private companies aim to make a profit, and public organizations do not. The result of the assessment is presented in figure 17.

Figure 17



A first observation that can be made using the presented figure is that for both private and public organizations, the downtime consideration seems to be successful in persuading the majority of surveyed professionals into advising or deciding to make a payment. However, as could be expected, this effect is stronger with private companies than with public organizations. The figure shows that only 28 percent of surveyed professionals argue that projected downtime would not influence their decision-making process. This means that a majority of 72 percent of private respondents would take projected downtime in their decision-making process and within this group, 42 percent would decide to make the ransom payment if the projected downtime is longer than a week, and around 19 percent would do this if the downtime is longer than three days and the smallest group of 11 percent would only decide to pay if it is expected that the downtime would be longer than a month. In the public sector, 43 percent of professionals respond that downtime does not influence their decision-making making process regarding payment, a larger group than in the private industry but still a minority. Just like in the private sector, the biggest group says that they would decide/advise to make the payment if the projected downtime is longer than a week.

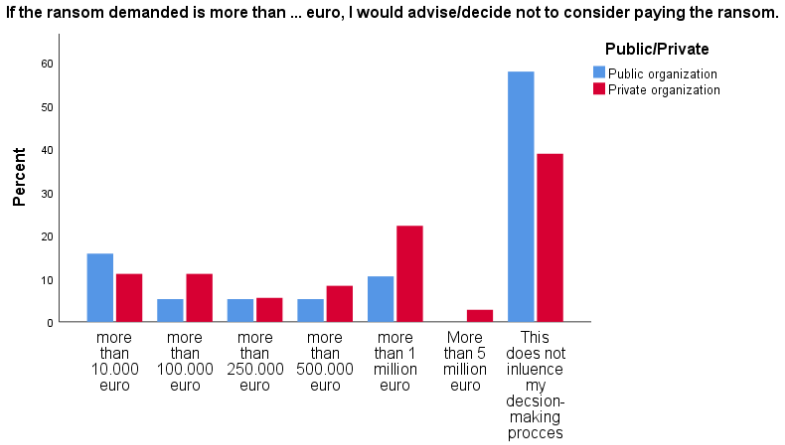
It seems that framing a ransomware scenario in terms of projected downtime instead of the direct costs connected to this has a positive effect on the likelihood of the respondents to decide to go with payment of a ransom demand. An explanation for this could possibly be found in that information- and cybersecurity professionals would think more in terms of the CIA (Confidentiality, Integrity, and Availability), and thus in the uptime of the systems they manage than the actual cost connected to the downtime of these systems.[71] This explanation is reinforced by the fact that when respondents were asked to provide an estimation of how much money the downtime of business processes would cost the organization per day, 81 percent of respondents answered that they could not come up with such an estimation.

While the data does show that if the projected downtime is longer than a week, a large part of respondents is prepared to pay a ransom demand, it is important to mention that paying for decryption does not necessarily mean that the downtime of the organization will be shorter. Decrypting a corporate network could take days or even weeks, and there is no guarantee that the decryptor will decrypt all the data flawlessly.[72] Paying for a decryption key does, therefore, not necessarily mean that an organization will experience shorter downtime than when it decides to repair their systems without a key.

[71] Forcepoint, 'What Is the CIA Triad?'
[72] 'Factsheet Ransomware - Nationaal Cyber Security Centrum'.

The data above shows that for a majority of the respondents extensive projected downtime serves as an incentive to decide/advise the making of a payment. However, as pointed out throughout this research, the decision to make a payment or not is a multifactor deliberation with lots of moving parts. In the conceptual part of this research, it was hypothesized that the actual amount of demanded ransom could be an important consideration in the equation. This idea was already partly disqualified by the considerations ranking, where the amount of ransom demanded placed second to last. However, a question regarding the ransom amount was included in the survey, and the data collected from this question does show some interesting insights. The question, visualized in figure 18, asked the respondents if there was a certain amount of ransom that was so high that it would stop them from even considering making payment.

Figure 18



The data show distinct differences between public and private organizations. The most notable difference is that a majority of around 60 percent of the surveyed public professionals answers that the amount of the ransom demand does not influence their decision-making process, which could mean that because they do not even consider the amount, it would be unlikely for this group to ever pay. Adding to that, the second biggest group of public officials respond that they will not even consider a ransom demand that is more than €10.000. This also makes payment unlikely, as the average ransom demand in Q1 of 2020 was estimated at around $111.000 by cybersecurity firm Coveware.[73]

For the private industry, a different picture arises, with around 40 percent of respondents arguing that they are not influenced in their decision-making process by the actual amount of ransom demanded. While this is a big group, it consequently also means that around 60 percent of private industry respondents have some kind of bargaining space in which they would consider making payment. What is remarkable is that for 25 percent of private organizations (the second-biggest private industry subgroup), this bargaining space in which payment can be considered reaches up to 1 million Euro. What this model shows is that private organizations are much more receptive to the possibility of payment than public organizations and that these organizations generally have more bargaining room to consider a certain amount of ransom.

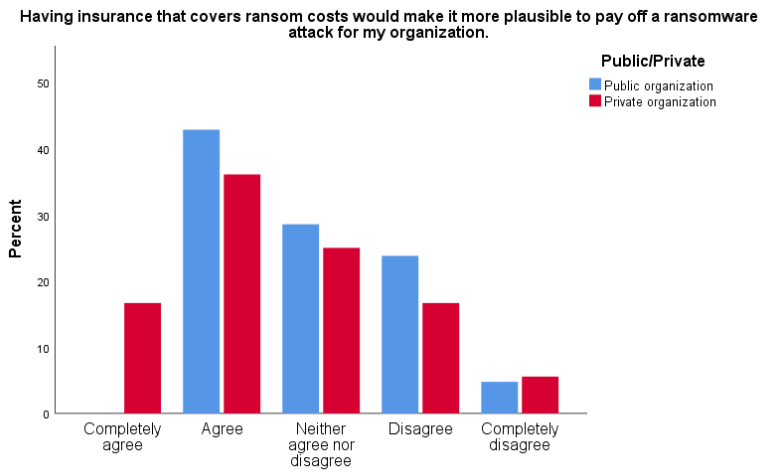
The analysis above described how economic and financial factors like projected downtime or the amount of the demanded ransomware do or do not influence the decision-making of the surveyed professionals. Another often heard factor in the discussion about the problem of targeted ransomware is the role of insurance companies. Cybersecurity vendor Sophos reports in their 'State of Ransomware 2020' report that 64 percent of Dutch companies have cybersecurity insurance that covers the cost ransomware.[74] It has been reported that, in some

[73] 'Ransomware Payments Up 33% As Maze and Sodinokibi Proliferate in Q1 2020'.
[74] SophosLabs, 'The State of Ransomware 2020'.

cases, insurance providers advise organizations to pay the ransom because they feel that going with this option will be the cheaper option.[75] Dutch Minister of Justice and Security Ferdinand Grapperhaus has already urged Dutch insurers to stop with covering payment of ransom because, according to him, this accounts for "actively aiding and abetting" criminal enterprises and he would rather see that insurers would pay for the recovery cost instead of urging companies to pay.[76]

It seems a logical assumption that the having of cybersecurity insurance would make it more plausible for organizations to pay a demanded ransom, as the organization would get their data back, and the insurer would pay the ransom demanded and the further cost that the ransomware incident would have caused. This assumption would at least be logical for private companies as the direct cost of a crisis would be more of a concern here with a government institution. Figure 19 shows that both in private as well as public organizations, most respondents say that it would make it more plausible for their respective organizations to pay a ransom demand if these costs would be covered by an insurance provider. This seems like a logical conclusion; however, it cannot be established using this data on how strong the incentive of the having of insurance that covers the payment of ransom actually is. The decision-making process regarding this decision is a multifactor equation, and while a positive effect is observed, it cannot directly be established that the having of ransomware insurance leads to payment also because it was shown earlier that this decision is not the result of a simple cost-benefit analysis.

Figure 19



The assessment of economic incentives subdimension has provided useful insight into what extent economic and financial incentives play a role during the crisis decision-making process of a ransomware scenario. What can be concluded is that the resolution of a ransomware crisis is not merely the result of conducting an economic cost-benefit analysis looking at the direct cost of paying or not paying. The surveyed professionals seem not to be incited by direct economic costs when forming their opinion about resolving a ransomware crisis. However, when the respondents are presented with the possibility of sustained downtime, they seem more receptive to consider the possibility of paying the ransomware actors. A majority of both private and public professionals indicated that if projected downtime of business processes in case of an independent repair operation is longer than a certain amount of time, they would advise or decide to make payment. For some respondents, this threshold is already reached after three days; others indicate that they can hold out for a month. However, the biggest groups, both in the public and private sectors, indicate that if the projected downtime is longer than a certain time, they will decide or advise to make payment. This being said, there remains both for public and private organizations, a relatively large group that argues that downtime does not influence their decision-

[75] Dudley, 'The Extortion Economy'.
[76] NRC, 'Grapperhaus wil dat verzekeraars losgeld aan hackers niet vergoeden'.

making. However, it can still be concluded that most respondents are more receptive to the threat of downtime as an incentive to pay than to the direct cost connected to this.

In analyzing if the amount of demanded ransom has an effect on the respondent's willingness to make a ransom payment or not, notable differences between the private and public sectors were found. The majority of public respondents indicated that the height of the ransomware amount did not influence their decision regarding payment, the second biggest group answered that they would not consider a payment higher than 10.000 euro, the lowest possible option. The private professionals showed to be more receptive to place the actual amount of demanded ransom in their decision-making process, with the biggest group of the surveyed respondents indicating that if the ransom demand surpassed one million euro, they would not consider making payment. This, of course, does not mean that a demanded ransom sum lower than one million automatically means that this group will consider paying. However, it does show that there is some kind of bargaining room, something much less observable with public officials.

4.6.3.3 Structure: Communication systems

During an uncertainty event like a ransomware attack, a substantial part of the crisis decision-making process is setting up a strategy for the crisis communication implications of the incident. As pointed out earlier, this strategy has an internal side, which goes into how different internal stakeholders communicate in order to mitigate the crisis as effectively as possible and, on the other side, an external communication strategy which sets out the narrative directed at the outside world. Dissecting internal crisis communication is, just like unraveling informal norms of hierarchy and authority explained earlier in this research, a hard phenomenon to grasp with the help of an online distributed self-completed questionnaire. It can be done more effectively using a semi-structured interview and a case study research design. However, Ballesteros and Kunreuther have pointed our that open and clear internal communication in both bottom-up and bottom-down streams are the key to successful crisis mitigation.[77] In the hierarchy and authority subdimension, it was already covered that respondents generally feel like their concerns are heard and taken seriously, and this shows at least in some way, that at least the bottom-up stream of communication is adequate in the organizations of the surveyed respondents. However, a true dissection of how internal crisis communication systems are shaped within Dutch organizations falls outside this study.

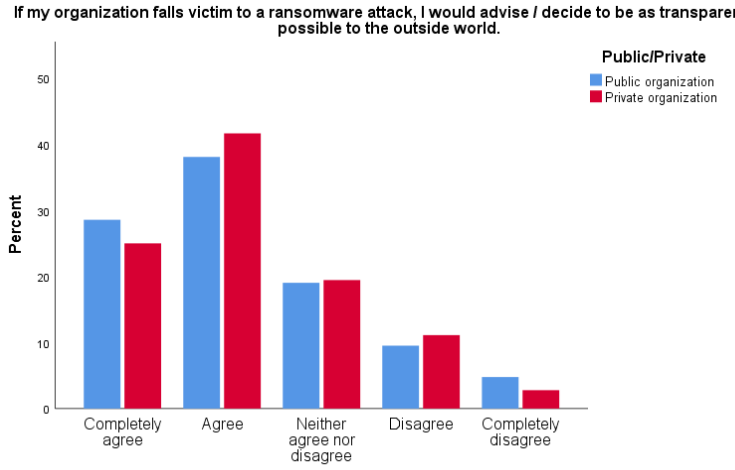
In this subsection, the considerations of our respondents regarding external communication will be discussed. As in the previous subsection, it was decided to provide the analysis with an extra layer by comparing the public and private sectors. In the analysis, the external communication component is largely understood as the appetite of the respondents to provide an open and transparent media strategy regarding the unfolding crisis. Recently Maastricht University and research institute Wetsus, two Dutch organizations previously hit with ransomware, called for more openness and transparency from organizations hit with ransomware because, according to them, openness and the sharing of experiences is the only way forward in mitigating the threat of targeted ransomware.[78] However, the road of transparency is not always easy, especially for private organizations, which are often afraid of reputational damage or legal implications.[79] However, in most ransomware cases, companies have to give some kind of insight into what happened because often the effects of an attack, like downtime. are notable for customers or other external stakeholders. However, the degree of openness and transparency that organizations give about a security incident like a ransomware attack differs greatly. Often organizations put out a public statement in which they refer to a ‘cyber incident’ and that the organization is ‘working towards

[77] Ballesteros and Kunreuther, ‘Organizational Decision Making Under Uncertainty Shocks’, 2018, 23.
[78] ‘“Slachtoffers van ransomware moeten meer openheid van zaken geven”’.
[79] ‘Class Action Lawsuit Filed against Two Puerto Rican Hospitals for Alleged Ransomware Attacks’.

fixing the problem' and keep it at that.[80] In other cases, like with the Maastricht University case, organizations react with total openness and transparency. The University went even so far to publish the extensive forensic report provided by Fox-IT, in order to help other organizations to learn from what happened to them.

In order to evaluate how our target population feels about transparency when dealing with a ransomware incident, the respondents were presented with the statement presented in figure 20. As one can examine in the figure, the respondents largely agree with the statement, and this indicates that they would always advise being as transparent as possible to the outside world, and there are no substantial differences between public and private organizations. This seems like a positive result that organizations are transparent about the hardships they faced when managing a ransomware crisis, and if they would share how they fell victim, the better other organizations can defend against and prepare for such an attack. However, it could be the case that for this question, respondents are answering in a socially desirable manner or that they are not the ones that make the decisions on this matter.

Figure 20

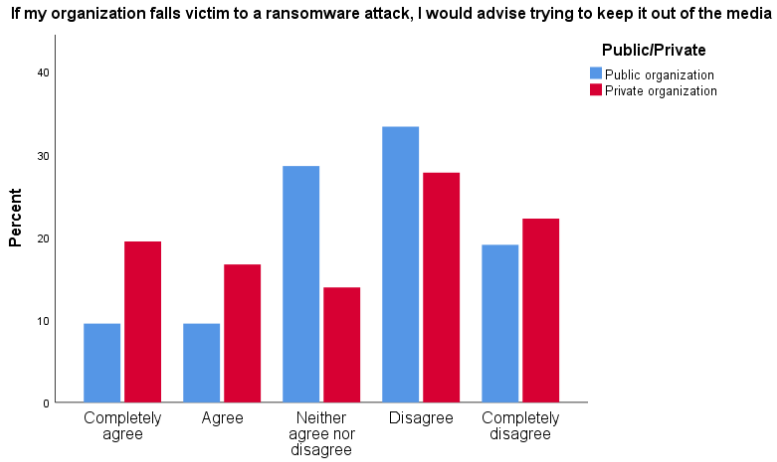


The reason for this idea is two-fold, first of all: although the Dutch police received 188 reports of ransomware cases in 2019 and almost 25 percent of the respondents of the survey pointed out that their organization had previously experienced ransomware, you can count the publicly known cases in the Netherlands on one hand. The majority of respondents indicate that they want to be "as transparent as possible to the outside world as possible" but looking at what we publicly know about ransomware cases in the Netherlands it seems that this is either an empty promise or that the questioned professionals do not have the authority to make this call. However, it could also be the case that organizations are indeed trying to be transparent, but the media does not deem the cases newsworthy and fails to report them.

What further deteriorates the claim the respondents are true proponents of openness and transparency is that when the respondents are asked about if they would to advise to keep a ransomware incident out of the media, as can be seen in figure 21, more than 35 percent of respondents in private organizations indicate that they indeed would try to keep the attack out of the media. For public organizations, around 20 percent agree with the statement, and 30 percent is undecided about the mater. While this still means that for both groups, around 50 percent would not try to keep the incident out of the media and would indeed try to opt for transparency, the data in figure 21 does show that this may be easier said than done.

[80] 'Travelex UK on Twitter'.

Figure 21



The fear of reputational damage could be an important factor in the consideration to keep a ransomware incident out of the media. The prevention of reputational damage was the fourth most important consideration in the ranking presented earlier and is thus arguably quite important in the decision-making process of the surveyed professionals. However, it should be noted that being open and transparent about the perils of a ransomware attack can lead to positive effects on an organization's reputation. An example: when Norwegian aluminum multinational Norsk Hydro was hit with ransomware and had to shut down 170 plants around the world, the management chooses to react with complete transparency and openness to its workforce and the outside world. The company took a proactive communication stance and opened up a temporary emergency website, which provided daily press releases and even webcasts where anybody could ask questions. The strategy was effective in countering rumors, and Hydro was able to resolve the crisis on their own initiative. Investors were pleased with this approach, and in the days after the incident, Hydro even saw a substantial stock rise.[81] In the end, Hydro chose not to negotiate with the criminals and did not pay a single bitcoin. However, because of the immense size of the infection, spreading across continents, Hydro estimates the total monetary impact of the attack at a staggering 75 million dollar.[82] While the attack on Norks Hydro will go into history as one of the most costly attacks ever, the communication strategy is widely praised and serves as a blueprint for other organizations.[83] While the respondents of the survey seem to hold back on providing true transparency in the event of a ransomware attack, the case of Hydro shows that secrecy and silence may not always be the best strategy.

4.7 Marco dimension

As discussed earlier, organizations do not operate in a vacuum of their own preferences, the social-economic and institutional context of an operating environment influences how organizations operate and shape their strategies. Furthermore, organizations are often dependent on vast stakeholder and supply-chain networks, which play an important role in business processes. To evaluate this environment around an organization, Ballesteros and Kunreuther have provided the Macro dimension, which consists of two subdimensions: *Institutions* and *Stakeholders*.

[81] Billbriggs, 'Hackers Hit Norsk Hydro with Ransomware. The Company Responded with Transparency'; 'Norsk Hydro'.
[82] 'Norsk Hydro Cyber Attack Could Cost up to $75m'.
[83] 'Hydro Awarded for Cyber-Attack Transparency'; 'In Its Ransomware Response, Norsk Hydro Is an Example for Us All'.

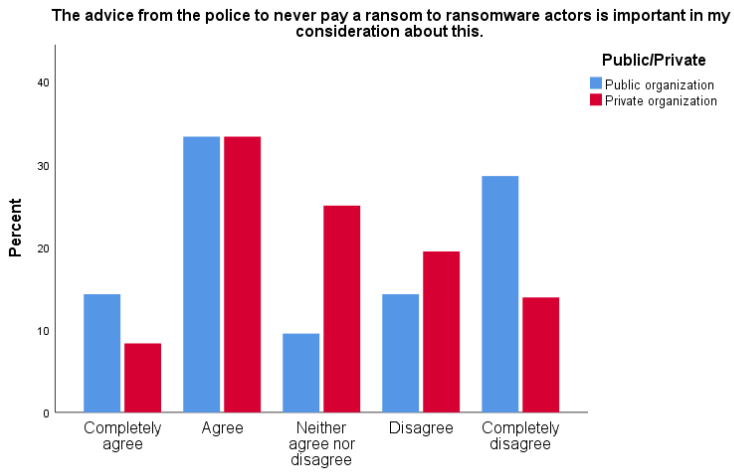
4.7.1 Institutions

In the Netherlands, there are no formal regulations or policies that set out how organizations should deal with a ransomware scenario, except for the reporting obligation to the Dutch Data Protection Authority if personal data was encrypted. The evaluation of the institutional environment influencing the decision-making process of organizations dealing with targeted ransomware will, therefore, be focused on the institutional pressure provided by the Dutch government to persuade organizations and consumers that fall victim to ransomware not to pay. In earlier parts of this research, it was already established that this advice from the Dutch government to never proceed to payment was the lowest consideration in the ranking. However, it was also established that there were some notable fluctuations between public and private organizations. In order to further explore the considerations of the respondents regarding the institutional pressure described, two questions about this matter were included in the survey. Because notable differences between public and private organizations could be expected regarding this matter, the models are split on this basis.

Figure 22 describes to what extent respondents feel the advice from the Dutch police to never make payment in a ransomware scenario is important in their consideration about this. As the consideration was ranked the lowest in the general ranking, an unambiguous result could be expected. However, as can be seen in the figure, this is not the case. Both for the public and private sector, the two biggest groups of 33 percent, agree with the posed statement and indicate that the advice from the police is thus fairly important in their decision-making process. While the consideration was last in the ranking, the biggest group of respondents still feels like the factor has some importance during the resolving of a ransomware crisis.

In an earlier part of this research, it was put forward that it would seem logical that this advice of the police would find more fertile ground within the public sector. However, this seems not to be the case; the second biggest group of public sector respondents 'completely disagree' with the posed statement. This is somewhat an unexpected result; it would seem more logical that private organizations would ignore institutional pressure like this, also because this advice is not only carried by the police but other influential government bodies like the NCSC. However, looking at the data, it seems that actually private organizations are more receptive to the message put out by the government.

Figure 22



While it was expected that the respondents would largely disregard the advice of the police in their decision-making process because of its low ranking compared to other considerations, the data in figure 22 does not reflect this suggestion. The data is drawn-out over the model and does not reflect a clear conclusion. For this reason, it is hard to provide a clear-cut conclusion about the effectiveness of the institutional pressure against payment coming from the Dutch government.

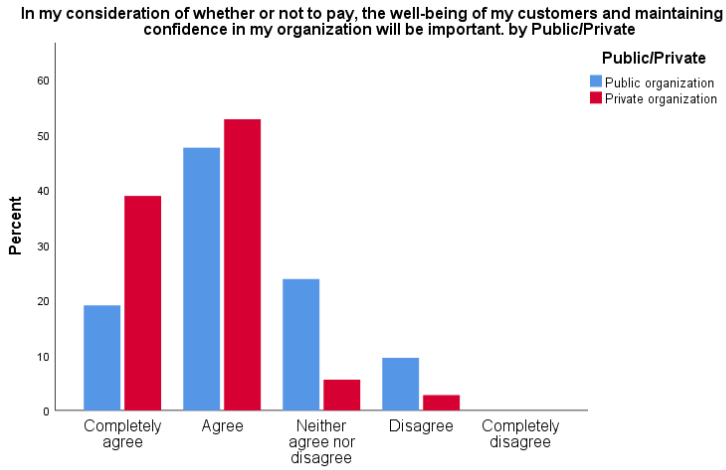
4.7.2 Stakeholders

It was pointed out earlier that the perils of a ransomware attack often not only influence the targeted organization but can have an extensive waterbed effect on customers, supply-chain partners, and other stakeholders involved. In terms of the ethicality of deciding to pay or not, the notion that payment of criminals is unethical sometimes directly conflicts with the fact that not paying can mean that numerous stakeholders outside the organizations can be severely damaged in their interests, something that could also be deemed unethical. In the after-action report of the University Maastricht, this conflict is clearly described as the board illustrates how the interests of students, researchers, and other staff members in terms of study progress, research and salary payments, weighted more heavily than the moral obligation to not aid and abet a criminal business model.[84]

Placing the interests of stakeholders above the ethical objections to pay can also be observed in the considerations ranking, as the mean score of stakeholder interest was more than 20 points higher than the score regarding the ethical objections of paying a criminal actor. For this reason, it is no surprise that for both public and private organizations, a significant majority agrees or completely agrees with the statement that the interests of customers will be important in the decision to make the payment or not. The same pattern of preferences was observed with the same question but then regarding the interests of chain-partners instead of customers.

What is clear is that organizations place the interests of external stakeholders high on their priority list when dealing with an uncertainty event like ransomware. This seems noble but is, of course, also the result of the self-interest of the organizations. If the customers of a private company are severely damaged in their interest and blame the management of a crisis like ransomware for this, the chances are high that this will lead to these customers terminating their relationship with the organization, leading to a decline in revenue for the company. The same goes, to some extent, for public organizations, if citizens are increasingly dissatisfied with the functioning of a public institution, this can lead to extensive democratic scrutiny.

Figure 23



4.8 Conclusion of data analysis

The analysis of the data collected using the survey has shown that the decision-making process during a ransomware crisis consists of lots of moving parts and that decision-makers have to take a vast amount of intertwined considerations into account when making decisions about how to resolve such a crisis. With the collected data, it was possible to establish a ranking in these considerations and establish what the priorities of the surveyed professionals are. Unsurprisingly, the factors regarding business continuity and customer interests outranked the other considerations firmly. More surprising results could be found at the bottom of the ranking, with the actual amount of a ransom demanded ranking second-to-last and the advice from the government and

[84] University of Maastricht, 'UM Cyber Attack Symposium – Lessons Learnt'.

law enforcement to never pay ransom ranking last. Looking at the differences of these consideration rankings between the public/private and vital/non-vital sectors, the general order of the considerations stayed the same, although some notable and interesting fluctuations were found in the actual scores given per sector. However, it was not able to establish statistical significance for most of these fluctuations, and these results should, therefore, be revisited using larger *n* empirical data and more extensive analysis.

The theoretical framework served as a useful tool to provide a clear structure for the deeper analysis of the collected data. Some subdimensions seemed more useful in dissecting the problem of targeted ransomware than others, but generally speaking, the framework was fitting for the analysis. The two dimensions, meso and macro, provided an outline to both consider the organizational level itself as well as the wider social-institutional context organizations operate in. With the collected data, it was not possible to assess the *Strategy* dimension in the exact way Ballesteros and Kunreuther conceptualized the subdimension, as it was not possible to find meaningful differences in how the organizations of the surveyed professionals formulated long- and short term goals. However, understanding the strategy dimension in terms of organizational differences between the public/private and vital/non-vital sectors, also led to profound analysis, as is described above.

The *Hierarchy and Authority* dimension provided some insight into the 'cybersecurity maturity' of the organizations for which the surveyed professionals are active. The data showed that generally speaking, the respondents feel that they are taken seriously and that their concerns will be translated into action when needed. However, the data also indicates that previously cybersecurity risks and vulnerabilities have been downplayed, taken for granted, or straight out ignored. Such a finding is not surprising; the agenda-setting of cybersecurity issues has always been a difficult avenue. However, the data shows that a majority of organizations for which the respondents are active have developed (and often practiced) crisis scenarios for the handling of a ransomware incident, showing that this threat has been put on the agenda successfully. Moreover, it could well be the case that high-profile incidents like the Maastricht case are causing an increased cybersecurity awareness among Dutch public and private organizations, because the realization of 'this could also happen to us' is finally sinking in.

Arguably the most extensively covered subdimension is *Economic Incentives*. This seems logical; in its core, ransomware is a criminal business model aimed at extorting victims for financial gains. However, the idea that the solution of a successful ransomware attack can be deducted from a simple cost-benefit analysis regarding the direct costs of paying or not seems not to be valid. The data indicates that even if paying the ransom is the cheaper option, this does not serve as a direct incentive to pay. This corresponds with the fact that the actual ransom sum and this sum in relation to an independent repair operation rank second- and third-to-last in the general considerations ranking. However, if the problem of ransomware is framed in terms of business continuity instead of direct costs, the professionals seem more receptive to consider payment. Both private and public professionals indicated that if the projected downtime of an independent restoration took longer than a certain amount of time, they would decide to make payment. For most professionals, this threshold was as short as a week. However, caution is required with this conclusion; making payment in order to acquire a decryptor and restoring systems using this solution could still take days or even weeks, and during this time, an organization will still experience downtime. Acquiring a decryptor is thus in no way a magic bullet that will fix an organization's problems in a few hours.

As pointed out earlier, the actual amount of ransom is low on the priority list of the respondents. However, it was still regarded as meaningful to see if, and if so, to what extent the professionals would take a certain amount of ransom demand into their decision-making process. The analysis found clear differences between public and private respondents regarding this matter. A majority of more than 60 percent of public respondents indicated that the amount of ransom did not influence their decision-making process, which could mean that they are

unlikely to pay in every scenario as they do not even consider the amount. The second biggest subgroup indicated they would not consider a payment higher than 10.000 euro, as in most cases the ransom demands are ten times as high, this group seems unlikely to make payment. On the other hand, private organizations seem to have more room for discussion on this matter. As more than two-thirds of private respondents indicate that they have some kind of maximum up until they would consider making payment, for most this number was 1 million euro, a steep difference with their public counterparts.

The last subdimension, *communication systems*, looked at communication and specifically at to what extent organizations will take the road of transparency and openness to the outside world when resolving a crisis like ransomware. While most respondents point out that they indeed like to provide transparency to the outside world, the data shows that a significant part of respondents also would advise keeping a ransomware incident outside the media if the organization they work for would hit with an attack. While openness is often preached, it seems that there are still some corners to take and that not everybody is adhering to the call for openness about ransomware incidents.

With the help of the *macro* dimension, the institutional pressure of the Dutch government to discourage victims of ransomware from making the payment was assessed. It was concluded that this effort should be regarded as not very efficient because this consideration is ranked by far lowest priority for the respondents. This conclusion should be a wake-up call for policy-makers; it seems that their efforts are not very effective, and it may be wise to rethink their strategy. The second element of the macro dimension described the importance of stakeholder interests in the decision-making progress of the surveyed professionals. Something that was already demonstrated in the consideration ranking, where this factor was placed on the third place of importance directly after the two business continuity factors.

The structural interpretation of the collected data in this chapter has proven that the decision-making process regarding ransomware is a multifactor deliberation with lots of moving parts. In the next chapter, the research question will be revisited in order to come up with a comprehensive answer to this question, this will, of course, be done, with help from the data interpretation provided in this chapter.

Conclusion

5.1 Introduction

In this concluding chapter, the research question posed in the first chapter of this study will be revisited and provided with a comprehensive answer. This research question that served as the starting point of this project is:

What considerations determine crisis decision-making in targeted ransomware scenarios, and how do these considerations influence the decision to pay the ransom or not?

By looking at this question, it can be argued that the first part of the question has been extensively covered; the analysis of the collected data has provided a thorough insight into the complex assemblage of different considerations that play their part during the mitigation of a ransomware crisis. Furthermore, in the analysis, it has been described how the surveyed professionals prioritize these different concerns and showed, unsurprisingly, that concerns regarding business continuity and stakeholder relations have the highest priority for the respondents. Furthermore, it was also found that the decision-making process of the respondents cannot be reduced to an economic cost-benefit analysis and that decisions will not be made by just going for the cheapest option. It was also found that institutional pressure coming from the Dutch government has little impact on the decision-making process of the question respondents and that transparency is not a priority for the respondents.

The study has thus provided an extensive overview of the different considerations at play during the multidimensional decision-making process of a targeted ransomware attack. This last chapter attempts to connect all these moving parts and describe the decision-making process from start to end. In order to do this, there will be a clear focus on the last part of the research question; the shaping of the decision to make the payment or not. As a tool to provide this analysis, a diagram providing a simplified visualization of the different considerations in the decision-making process about making the payment or not has been outlined in appendix 4. In this chapter, the decision-tree will be followed through and combined with the insights from the theoretical and empirical insights described earlier. However, it should be noted that the visualized decision-tree is a simplified interpretation of this process and should not be seen as an exact and generalizable reflection of the real-world. Furthermore, it should be emphasized that this model and analysis looks at the actual decision-making process regarding making the payment or not and that previously covered conditions and circumstances like the preparedness and chosen communication strategy of an organization is not part of this analysis.

In order to lift the research out of the hypothetical sphere, the decision-tree will be assessed with the help of examples from the decision-making process of a real-world case. This case is the earlier described Maastricht University (UM) ransomware incident that took place during the last two weeks of December 2019. The reason that this case is chosen is that the decision-making process of this crisis has been extensively documented in a public report provided by Fox-IT and the UM and that the Dutch Inspection for Education has provided an independent and in-depth report that describes the decision-making process of the UM in great detail.[85] This kind of transparency is unusual for ransomware incidents, and it would be a missed opportunity not to use these insights to make the collected data and analysis of this study come to life.

[85] Ministerie van Onderwijs, 'Rapport Cyberaanval Universiteit Maastricht'.

5.2 To pay or not to pay?

As with all cyberattacks, ransomware has an extensive 'kill-chain' starting with reconnaissance, initial access, lateral movement, and moving up towards the actual decryption and making a ransomware demand.[86] The end of this kill-chain is the start of this study; the data is encrypted, and an organization's IT infrastructure is likely to be largely unavailable. As described earlier, the most important factor for a ransomware incident to qualify as an organizational crisis is that the incident threatens the continuation of vital business processes and, in this way, the high priority goals of an organization.[87] If this is not the case, the incident can be contained and fixed without large problems and logically does not spark a crisis.

The first step of dealing with a ransomware incident is thus assessing the scope of the attack, and asking the question: are my vital process at harm and is there vital data encrypted? In the Maastricht case, this assessment was quickly made. On the 23rd of December, the day before Christmas, the ransomware incident is discovered as administrators find themselves locked out of their systems, and different university services like the email systems go offline. The University's CERT quickly realizes that they are dealing with a serious incident and decides to isolate the network, close all University buildings, call in the help of Fox-IT and notify the board.[88] The next day the first meeting of the crisis management team (CMT) is held, composed of different C-level executives, specialists, and the incident responders from Fox-IT.[89] At this moment, it is clear that an extensive ransomware attack has hit the UM, and although the incident occurred during the holidays, it is evident that the University is hindered in its primary and core process: the ability to provide education and conduct research.

The report provided by the Inspection for Education describes how the CMT, in their decision-making process, drew up three different scenarios to explore towards resolving the crisis. First, there was the idea to build a decryption solution that could be used to decrypt the compromised systems without the involvement of the criminals holding the UM hostage. This scenario was followed up by Fox-IT, but it was assessed that this option was not feasible. Even if the undertaking would be successful, the disruption of educational and research activities was estimated at three months, and this was unacceptable to the UM.[90]

With the self-provided decryption solution not delivering a feasible way out of the crisis, the CMT had to consider the second option: restoring the compromised network themselves and falling back on backups, an option also described in the decision-three in appendix 4. However, going with this option would lead to numerous unacceptable implications for the University. First, it was assessed that going with this option would lead to a disruption of primary processes of between two and three months. Furthermore, it was unclear whether or not going with this option would mean that all data could be restored.[91] The reason for this was that the university mainly used 'online' backups, which means that the backup systems are, in some way, connected to the network, which means that an attacker with the right administrator privileges can encrypt these backup servers. It was assessed by Fox-IT that this was indeed the case for some servers and that for this reason, total data recovery could not be guaranteed.[92] Lastly, it was also the case that the university had not practiced the recovery of backups and that for this reason, such an undertaking would be extra timely.[93]

[86] Dargahi et al., 'A Cyber-Kill-Chain Based Taxonomy of Crypto-Ransomware Features'.
[87] Hermann, *International Crises*.
[88] Ministerie van Onderwijs, 'Rapport Cyberaanval Universiteit Maastricht', 22.
[89] Ministerie van Onderwijs, 23.
[90] Ministerie van Onderwijs, 23.
[91] Ministerie van Onderwijs, 23.
[92] Fox-IT, 'Spoedondersteunig Project Fontana', 21.
[93] Fox-IT, 33.

The option to restore the systems without a decryption solution was thus in conflict with the two highest-ranked considerations part of the empirical part of this study, the loss of crucial data and the prevention of long-term business stoppages. The decision to go with payment is also in line with the observation a lot of the respondents indicate that if the projected downtime in connection to an independent conducted restoration operation is longer than a certain time - a week for most - they would choose to pay the demanded amount. As concluded earlier, the threat of downtime of vital business processes together with data loss thus serves as the most crucial incentive for ransomware victims to pay. And this is the case especially with the UM case because downtime and data loss directly conflict with the interests of the most important stakeholders for the UM, its students, and academic staff.

For reasons stated above, the CMT thus determined that paying the hostage-takers had to be explored. Before doing so, the UM obtained external legal advice about getting in contact with the hostage-takers and informed the police about doing so.[94] The considerations of the university regarding the unethicality of paying criminal actors and the advice from the Dutch government to never pay such actors are described clearly in the report of the Inspection for Education. The report describes how the UM completely endorses the notion of the unethicality of paying criminal actors and is aware that supporting these criminal enterprises helps to keep them in business and that this is thus against the public interest. However, during the crisis, UM made the assessment that the public interest was subordinate to the interest of the institution because of the obligations that the university had to its students and academic staff.[95] This conclusion is also reflected in the findings of this study; respondents regard paying demanded ransom as an unethical practice but also indicated that at some point, the concerns of business continuity and stakeholder interests outweigh these ethical obligations.

The fear of months of disruption of educational activities and the possibility of losing scientific data forever made the UM decide that payment was the only solution to their problem. Before the university wanted to make the payment, some assurances were sought. First, the university transferred a number of files to the hostage-takers, who sent them back decrypted to prove that they could indeed decrypt the files. Second, the university transferred small amounts of Bitcoins (BTC) to the provided address and asked the criminals to answer how much they received, in order to make sure that they would send the demanded amount of 30 BTC - around 198.000 euro - to the right crypto address.[96] What also helped in establishing trust was that Fox-IT was able to attribute that attack to the well-known threat actor TA505, who had already made 150 victims until that time and that there was a high amount of certainty that if payment was made the group would indeed provide a decryptor.[97] Using multiple ways to authenticate the attacker or having an idea of the group thus seems to serve as a reinforcing factor for payment.

The amount that was demanded is a large sum of money, but it also falls within the boundaries of what most respondents of this study regard as acceptable when they would consider making payment. The report states that the Inspection regards the amount as ‘expedient’ because the calculations showed that hiring an external specialist to rebuild the infrastructure in combination with the cumulative liability towards students was far more costly than paying the demanded amount.[98] However, it should be noted that there is no evidence in the report that the decision to pay was made because of this cost estimate. The university was not insured against cyber incidents like ransomware and had to pay the demanded amount out of own liquidity but was able to do so by using dividend from a separate university holding that recently had sold a start-up. By using this

[94] Ministerie van Onderwijs, ‘Rapport Cyberaanval Universiteit Maastricht’, 23.
[95] Ministerie van Onderwijs, 24.
[96] Ministerie van Onderwijs, 24.
[97] Fox-IT, ‘Spoedondersteunig Project Fontana’, 26.
[98] Ministerie van Onderwijs, ‘Rapport Cyberaanval Universiteit Maastricht’, 24.

construction, there were thus no direct public subsidies used to make the payment, which could have been an objection for a semi-public organization like the UM.[99]

After the payment was made, the university indeed received working a decryptor and was able to recover its systems. On the 6th of January, when the university resumed after the holidays, the university was able to run its core business as usual, and education and research resumed. In the end, only a handful of complaints were received by the university of students who argued that their study progress was affected in a negative way. The Inspection report concludes that the UM was not fittingly prepared for a ransomware incident and that there were some serious problems with the defensive measures taken by the University. However, it is also concluded that the crisis management decisions made by the UM deserve appreciation, and the Inspection agrees with the decision of the board to place the interests of the students and scientific staff above the ethicality of paying the ransom to a criminal enterprise.[100]

This conclusion also seems to be fitting when looking at the results of this study. The considerations that have been taken into account during a ransomware crisis are extensive and difficult. People do not want to be extorted, and it is clear that payment is an undesirable and unethical last resort. However, this undesirability can be outweighed when the business continuity of an organization is seriously threatened, and when the interests of stakeholders like customers are at stake. This inconvenient truth is exactly what makes the ransomware business model so successful and not likely to go away in the foreseeable future.

5.3 What can be done?

With the practice of 'big game hunting' not going away in the foreseeable future, it is of utmost importance that organizations mature in their cybersecurity practices and that general awareness about the threat of targeted ransomware grows. In this last section of the study, some ideas, methods, and practices that can help organizations prevent, detect, and respond to ransomware attacks will be recommended. Furthermore, some suggestions will be made regarding the policy implications of dealing with ransomware and, lastly, the future research avenues regarding the threat of targeted ransomware will be explored.

Like is often the case with matters regarding (cyber)security, it is important to have a 'security aware' staff that has, at least to some extent, been trained to detect possible malicious activities like phishing. Like with lots of ransomware incidents, the UM case initial compromise started with an employee opening a phishing mail with an Excel file that had a malicious macro attached to it.[101] By providing periodic security awareness sessions to employees, serious gains can be made in the security posture of an organization. However, while the 'human as the weakest link' narrative is one that is quite strong throughout the cybersecurity community, it should be noted that serious cybersecurity matureness of an organization is not achieved by only providing security awareness training to the employees of an organization. And that other technical and non-technical means should be supplemented in order to put up a serious defense against ransomware actors.

In the report describing the UM case, Fox-IT provides a selection of recommendations that could have prevented the attack on the UM. These recommendations are quite generic and can thus be taken as advice for most organizations. First of all, it should not be made easy for attackers to move laterally through a compromised enterprise. This means that where possible, the network should be divided into different segments that need different privileges and credentials to be accessed and used. If this is done properly, the spreading of ransomware throughout an organization will be a lot harder.

[99] Ministerie van Onderwijs, 25.
[100] Ministerie van Onderwijs, 'Rapport Cyberaanval Universiteit Maastricht'.
[101] Fox-IT, 'Spoedondersteunig Project Fontana'.

Connected to this is that good patch and vulnerability management is essential. What this means is that there are processes in place that keep track of the different pieces of soft- and hardware running on the network and that when security vulnerabilities are found for these systems, they are patched as soon as possible. On the UM network, there were numerous servers vulnerable for the infamous EternalBlue exploit, that was developed by the NSA and later leaked by the unknown group the 'Shadow Brokers.'[102] While there has been a patch available since mid-2017, this patch was not installed on some servers of the UM, and this potentially made movement around the network easier for the attackers.[103] Having patch and vulnerability management in order is thus important but gets harder as networks grow and a variety of different systems that have to work intertwined with each other, especially in an 'open' environment like at a university.

Another important measure that is put forward by Fox-IT is the implementation of a Security Information and Event Management (SIEM) solution. By using such a solution, an organization is able to monitor its network and scan logs for anomalies.[104] By doing this, malicious actors can be detected early, and defensive measures can be taken. Since the incident, the UM has established a so-called Security Operation Center (SOC), where all this information is collected, and action is taken if needed. However, it should be noted that the implementation and managing of such a system requires substantial investment as well as specific knowledge and skills and is therefore not achievable for every organization. However, it is possible to outsource such services to external providers and, in this way, still enjoy this extra level of security.

The last line of defense in case of a ransomware attack should be, as one can expect, solid back-up systems. However, ransomware operators are getting more and more skilled in also compromising the systems that make these back-ups because often this back-up system is, one way or another, connected to the main network, this was also the case in the UM case.[105] To be better protected, it is therefore important to also have 'offline' back-ups, which are not connected to the network and are therefore safe from compromise. However, the keeping of an extensive offline backup of an organization's infrastructure is an expensive and time-consuming undertaking, especially with larger networks. It should also be noted, that the restoration of these systems from offline back-ups in case of a ransomware incident will be a time-consuming effort and that restoring from back-ups is not an à la minute fix.

If all the above fails and an organization is hit with a successful ransomware attack, it is important to have tailored, tested, and practiced crisis management procedures in place. As this study describes, an organization has to take a wide variety of considerations into account, and decisions need to be taken swiftly. Knowing beforehand how the decision-making process during a ransomware incident will look and knowing the stance of the organization on certain (ethical) considerations will make the crisis management more effective and will reduce the impact of a ransomware incident drastically. An effective crisis management procedure also needs to have a periodically practiced 'data recovery' plan, which describes which critical systems are to be restored first to secure business continuity as much as possible. By practicing such scenarios, the organization gets a feel for restoring from offline back-ups, which will increase efficiency during an actual incident.

On the policy level, it is clear that the current strategy of discouraging payment coming from law enforcement agencies like the Dutch National Police and EUROPOL is not very effective, as this factor ranks the lowest on in the considerations ranking of the questioned cybersecurity professionals. While it is understandable that law

[102] Avast, 'What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?'
[103] Fox-IT, 'Spoedondersteunig Project Fontana', 31.
[104] Fox-IT, 31.
[105] ZDNet, 'Ransomware Victims Thought Their Backups Were Safe. They Were Wrong'; Fox-IT, 'Spoedondersteunig Project Fontana'.

enforcement agencies take this stance, it can be recommended that these agencies at least partly rethink their strategy. An interesting avenue for exploration on this matter is the possibility of deeper integration of the sharing of actionable threat intelligence about ransomware operators, either on a sectoral level, through for instance SURFcert for educational institutions, at the national level, through the NCSC or the Digital Trust Center or even the European level via the EUROPOL, possibly by expanding the mandate of an in-place structure like NoMoreRansom or the European Cybercrime Center EC3. While such institutionalization of information sharing is, of course, easier said than done, it should be noted that TA505, the group that attacked the UM, had previously attacked Antwerpen University. However, this information did not reach the UM in time and did thus not lead to extra vigilance.[106]

In terms of future research into the subject, it is clear that there is enough to investigate further as this study is only a first exploration into the crisis management implications of dealing with the threat of targeted ransomware. For every dimension and subdimensions covered throughout the analysis, there are interesting research avenues that can be further explored and dissected. For instance, research into different communication strategies during ransomware crises could provide useful insights. Also, much is still unclear about what strategies are actually effective in securing business continuity when an organization is hit with a ransomware incident, and more academic foundation into this would be useful. Lastly, attention should be paid to the institutional answer to ransomware, as it is clear that the current 'just don't pay' narrative is just not cutting it. Therefore, it should be explored how government entities, possibly through public-private partnerships, could come up with a more compelling answer to the threat of targeted ransomware, as it is clear that COVID-19 is not the only pandemic rattling the world at this moment.

[106] Ministerie van Onderwijs, 'Rapport Cyberaanval Universiteit Maastricht', 24.

Bibliography

Twitter. '(1) Travelex UK on Twitter: "Statement on IT Issues Affecting Travelex Services Https://T.Co/RpKagJLykn" / Twitter'. Accessed 8 July 2020. https://twitter.com/travelexuk/status/1212840156480315401/photo/1.

Autoriteit Persoonsgegevens. 'Datalek door ransomware: wat moet u doen?' Accessed 24 May 2020. https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/datalek-door-ransomware-wat-moet-u-doen.

Avast. 'What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?' Avast, 2020. https://www.avast.com/c-eternalblue.

Ballesteros, Luis, and Howard Kunreuther. 'Organizational Decision Making Under Uncertainty Shocks'. Cambridge, MA: National Bureau of Economic Research, 2018. https://doi.org/10.3386/w24924.

Billbriggs. 'Hackers Hit Norsk Hydro with Ransomware. The Company Responded with Transparency'. Transform, 16 December 2019. https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/.

Bryman, Alan. *Social Research Methods* (version 4). 4th ed. OUP Oxford, 2012.

Cartwright, Anna, and Edward Cartwright. 'Ransomware and Reputation'. *Games* 10, no. 2 (2019): 26. https://doi.org/10.3390/g10020026.

Choi, Jin Nam, Sun Young Sung, and Myung Un Kim. 'How Do Groups React to Unexpected Threats? Crisis Management in Organizational Teams'. *Social Behavior and Personality: An International Journal* 38, no. 6 (1 July 2010): 805–28. https://doi.org/10.2224/sbp.2010.38.6.805.

CyberScoop. 'Class Action Lawsuit Filed against Two Puerto Rican Hospitals for Alleged Ransomware Attacks', 13 February 2020. https://www.cyberscoop.com/hospital-pavia-class-action-lawsuit-ransomware/.

Dargahi, Tooska, Ali Dehghantanha, Pooneh Nikkhah Bahrami, Mauro Conti, Giuseppe Bianchi, and Loris Benedetto. 'A Cyber-Kill-Chain Based Taxonomy of Crypto-Ransomware Features'. *Journal of Computer Virology and Hacking Techniques* 15, no. 4 (1 December 2019): 277–305. https://doi.org/10.1007/s11416-019-00338-7.

'Data Analysis - Independent Samples t-Test'. Accessed 29 June 2020. http://learntech.uwe.ac.uk/da/Default.aspx?pageid=1438.

Dionne, Shelley D., Janaki Gooty, Francis J. Yammarino, and Hiroki Sayama. 'Decision Making in Crisis: A Multilevel Model of the Interplay between Cognitions and Emotions'. *Organizational Psychology Review* 8, no. 2–3 (May 2018): 95–124. https://doi.org/10.1177/2041386618756063.

Dudley, Renee. 'The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks'. ProPublica, 2019. https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks?token=TuMy8gExpvZxdxiWRs7mTz21zSyVml5E.

Edwards, Adrian, and Glyn Elwyn. 'Inside the Black Box of Shared Decision Making: Distinguishing between the Process of Involvement and Who Makes the Decision'. *Health Expectations* 9, no. 4 (2006): 307–20. https://doi.org/10.1111/j.1369-7625.2006.00401.x.

Forcepoint. 'What Is the CIA Triad?' Forcepoint, 9 August 2018. https://www.forcepoint.com/cyber-edu/cia-triad.

Fox-IT. 'Spoedondersteunig Project Fontana'. Fox-IT, 2 May 2020. https://www.maastrichtuniversity.nl/file/foxitrapportreactieuniversiteitmaastrichtpdf.

Fox-IT. 'WastedLocker: A New Ransomware Variant Developed By The Evil Corp Group'. *Fox-IT International Blog* (blog), 23 June 2020. https://blog.fox-it.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/.

Metro. ‘Garmin Obtains Decryption Key after Ransomware Attack’, 28 July 2020. https://metro.co.uk/2020/07/28/garmin-obtains-decryption-key-ransomware-attack-13046988/.

GCN, 2020. ‘NY Proposes Outlawing Ransomware Payments -’. GCN, 2020. https://gcn.com/articles/2020/01/27/ny-bill-bans-ransom-payments.aspx.

1Limburg | Nieuws en sport uit Limburg. ‘Groot Cyberhack Bij UM: “Criminele Aanval Niet Uitgesloten”’, 24 December 2019. https://www.1limburg.nl/groot-cyberhack-bij-um-criminele-aanval-niet-uitgesloten.

Hermann, Charles F. *International Crises: Insights from Behavioral Research*. New York, NY : London: The Free Press ; Collier-MacMillan, 1972.

‘Home NL - Cip-Overheid’. Accessed 15 July 2020. https://www.cip-overheid.nl/.

Hot for Security - Bitdefender. ‘Developer Hacks Back Against Ransomware Attackers and Steals...’ *HOT for Security* (blog), 9 October 2019. https://hotforsecurity.bitdefender.com/blog/developer-hacks-back-against-ransomware-attackers-and-steals-decryption-keys-21605.html.

‘Hydro Awarded for Cyber-Attack Transparency’. Accessed 10 July 2020. https://www.hydro.com/en-NO/media/news/2019/hydro-awarded-for-cyber-attack-transparency/.

Graham Cluley. ‘In Its Ransomware Response, Norsk Hydro Is an Example for Us All’, 3 April 2019. https://www.grahamcluley.com/in-its-ransomware-response-norsk-hydro-is-an-example-for-us-all/.

‘Internet Crime Complaint Center (IC3) | High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations’. Accessed 21 February 2020. https://www.ic3.gov/media/2019/191002.aspx.

Jupp, Victor. *The SAGE Dictionary of Social Research Methods: Volunteer Sampling*. 1 Oliver’s Yard, 55 City Road, London England EC1Y 1SP United Kingdom: SAGE Publications, Ltd, 2011. https://doi.org/10.4135/9780857020116.

Kahneman, Daniel author. *Thinking, Fast and Slow*. London: Penguin Books, 2012.

Kenton, Will. ‘Why Statistical Significance Matters’. Investopedia, 2020. https://www.investopedia.com/terms/s/statistically_significant.asp.

Kunreuther, Howard, and Michael Useem. *Mastering Catastrophic Risk: How Companies Are Coping with Disruption*. Oxford University Press, 2018.

Li, Yan, Neal M. Ashkanasy, and David Ahlstrom. ‘The Rationality of Emotions: A Hybrid Process Model of Decision-Making under Uncertainty’. *Asia Pacific Journal of Management* 31, no. 1 (March 2014): 293–308. https://doi.org/10.1007/s10490-012-9341-5.

Loman, Mark. ‘How Ransomware Attacks: What Defenders Should Know about the Most Prevalent and Persistent Malware Families’. SophosLabs, November 2019. https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-ransomware-behavior-report.pdf.

Maastricht University. ‘Cyberaanval - Een Samenvatting’, 2020. https://www.maastrichtuniversity.nl/nl/cyberaanval-een-samenvatting.

Mathijs Dijkstra, and Maarten van Dantzig. ‘Spoedondersteunig Project Fontana’. Fox-IT, 5 February 2020. https://www.maastrichtuniversity.nl/file/foxitrapportreactieuniversiteitmaastrichtpdf.

Ministerie van Justitie en Veiligheid. ‘Vitale infrastructuur - Nationaal Coördinator Terrorismebestrijding en Veiligheid’. Onderwerp. Ministerie van Justitie en Veiligheid, 24 April 2019. https://www.nctv.nl/onderwerpen/vitale-infrastructuur.

Ministerie van Onderwijs, Cultuur en Wetenschap. ‘Antwoord op Kamervragen over het bericht over cyberaanval Universiteit Maastricht - Kamerstuk - Rijksoverheid.nl’. Kamerstuk, 14 February 2020. https://www.rijksoverheid.nl/documenten/kamerstukken/2020/02/14/antwoord-op-kamervragen-over-het-bericht-cyberaanval-universiteit-maastricht-duurt-mogelijk-tot-na-de-kerstvakantie.

Ministerie van Onderwijs, Cultuur en Wetenschap. ‘Rapport Cyberaanval Universiteit Maastricht’. 31 May 2020. https://www.rijksoverheid.nl/documenten/kamerstukken/2020/06/12/definitief-rapport-cyberaanval-universiteit-maastricht-21pj-docx.

Morse, Edward A, and Ian Ramsey. ‘Navigating the Perils of Ransomware’. *Business Lawyer* 72, no. 1 (2016): 19.

Nationaal Cyber Security. ‘Factsheet Ransomware - Factsheet - Nationaal Cyber Security Centrum’. Publicatie. Nationaal Cyber Security Centrum, 26 June 2020. https://www.ncsc.nl/documenten/factsheets/2020/juni/30/factsheet-ransomware.

Nationaal Cyber Security Centrum. ‘Cybersecuritybeeld Nederland (CSBN) 2020’. Nationaal Cyber Security Centrum, 29 June 2020. https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020.

Nationale Politie. ‘Politie: 'Niet betalen bij ransomware’’. Accessed 24 May 2020. https://www.politie.nl/nieuws/2020/februari/6/00-politie-%E2%80%98niet-betalen-bij-ransomware.%E2%80%99.html.

NU. ‘NCSC: “Tientallen Nederlandse bedrijven getroffen door ransomware”’, 28 November 2019. https://www.nu.nl/tech/6014036/ncsc-tientallen-nederlandse-bedrijven-getroffen-door-ransomware.html.

ComputerWeekly.com. ‘Norsk Hydro Cyber Attack Could Cost up to $75m’. Accessed 10 July 2020. https://www.computerweekly.com/news/252467199/Norsk-Hydro-cyber-attack-could-cost-up-to-75m.

Dark Reading. ‘Norsk Hydro: This Is How You React to a Ransomware Breach’. Accessed 10 July 2020. https://www.darkreading.com/application-security/ransomware/norsk-hydro-this-is-how-you-react-to-a-ransomware-breach/a/d-id/750396.

NRC. ‘Grapperhaus wil dat verzekeraars losgeld aan hackers niet vergoeden’. *NRC*, 2020. https://www.nrc.nl/nieuws/2020/04/22/grapperhaus-wil-dat-verzekeraars-losgeld-aan-hackers-niet-vergoeden-a3997574.

Dagblad van het Noorden. ‘Openheid beste verdediging tegen ransomeware-aanval’. Accessed 1 June 2020. https://www.dvhn.nl/economie/Ransomware-Openheid-helpt-25354513.html.

Palmer, Danny. ‘What Is Ransomware? Everything You Need to Know about One of the Biggest Menaces on the Web’. ZDNet, 2018. https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/.

Pearson, Christine, and Judith Clair. ‘Reframing Crisis Management’. *The Academy of Management Review* 23, no. 1 (1998): 59–76. https://doi.org/10.2307/259099.

Pramanik, Roshni, Olof Ekman, Henrik Hassel, and Henrik Tehler. ‘Organizational Adaptation in Multi-Stakeholder Crisis Response: An Experimental Study: Organizational Adaptation in Multi-Stakeholder Crisis Response: An Experimental Study’. *Journal of Contingencies and Crisis Management* 23, no. 4 (December 2015): 234–45. https://doi.org/10.1111/1468-5973.12094.

‘Ransomware Infecteert Systemen Universiteit Maastricht - Security.NL’. Accessed 20 February 2020. https://www.security.nl/posting/636630/Ransomware+infecteert+systemen+Universiteit+Maastricht.

Coveware: Ransomware Recovery First Responders. ‘Ransomware Payments Up 33% As Maze and Sodinokibi Proliferate in Q1 2020’, 2020. https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report.

Emsisoft | Security Blog. ‘Report: The Cost of Ransomware in 2020. A Country-by-Country Analysis’, 11 February 2020. https://blog.emsisoft.com/en/35583/report-the-cost-of-ransomware-in-2020-a-country-by-country-analysis/.

Rittinghouse, John W. *Business Continuity and Disaster Recovery for Infosec Managers*. Amsterdam ; Boston: Elsevier Digital Press, 2005.

Security Boulevard. ‘Despite Increased Attacks, Security Remains Low Priority for Business’. Security Boulevard, 2019. https://securityboulevard.com/2019/03/despite-increased-attacks-security-remains-low-priority-for-business/.

Security Boulevard. ‘SHARED INTEL: How Ransomware Evolved from Consumer Trickery to Deep Enterprise Hacks’. Security Boulevard, 21 June 2020. https://securityboulevard.com/2020/06/shared-intel-how-ransomware-evolved-from-consumer-trickery-to-deep-enterprise-hacks/.

Opgelicht?! - AVROTROS programma over oplichting en fraude en bedrog. ‘“Slachtoffers van ransomware moeten meer openheid van zaken geven”’. Accessed 8 July 2020. https://opgelicht.avrotros.nl/alerts/artikel/slachtoffers-van-ransomware-moeten-meer-openheid-van-zaken-geven/.

SophosLabs. ‘The State of Ransomware 2020: Results of an Independent Study of 5,000 IT Managers across 26 Countries’, 2020. https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-ransomware-behavior-report.pdf.

TechRadar, and 2016. ‘A Helping Hand with a Dirty Trick: Ransomware Now Offers Helpdesk to Victims’. TechRadar. Accessed 21 February 2020. https://www.techradar.com/news/internet/a-helping-hand-with-a-dirty-trick-ransomware-now-offers-helpdesk-to-victims-1319034.

‘The No More Ransom Project’. Accessed 28 July 2020. https://www.nomoreransom.org/en/ransomware-qa.html.

‘Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware | U.S. Department of the Treasury’. Accessed 28 July 2020. https://home.treasury.gov/news/press-releases/sm845.

‘Universiteit Maastricht kampt met ransomware-aanval’. Accessed 20 February 2020. https://nos.nl/l/2316120.

University of Maastricht. ‘UM Cyber Attack Symposium – Lessons Learnt’. Symposium, 5 February 2020. https://www.maastrichtuniversity.nl/um-cyber-attack-symposium-%E2%80%93-lessons-learnt.

‘Update: Cyber Attack at UM #2’, 27 February 2019. https://www.maastrichtuniversity.nl/news/update-cyber-attack-um.

Valeriano, Brandon. ‘The Failure of Academic Progress in Cybersecurity’. Council on Foreign Relations, 2020. https://www.cfr.org/blog/failure-academic-progress-cybersecurity.

Waddell, Kaveh. ‘The Computer Virus That Haunted Early AIDS Researchers’. The Atlantic, 10 May 2016. https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/.

ZDNet. ‘At Least 13 Managed Service Providers Were Used to Push Ransomware This Year’. ZDNet. Accessed 26 May 2020. https://www.zdnet.com/article/at-least-13-managed-service-providers-were-used-to-push-ransomware-this-year/.

ZDNet. ‘Company Shuts down Because of Ransomware, Leaves 300 without Jobs Just before Holidays’, 2020. https://www.zdnet.com/article/company-shuts-down-because-of-ransomware-leaves-300-without-jobs-just-before-holidays/.

ZDNet. ‘Ransomware Victims Thought Their Backups Were Safe. They Were Wrong’. ZDNet, 2020. https://www.zdnet.com/article/ransomware-victims-thought-their-backups-were-safe-they-were-wrong/.

ZDNet. ‘Why Is It so Hard for Us to Pay Attention to Cybersecurity?’ ZDNet, 2019. https://www.zdnet.com/article/why-is-it-so-hard-for-us-to-pay-attention-to-cybersecurity/.

Appendices

Appendix 1: Terms and conditions survey

INFORMATIE EN TOESTEMMING

U wordt uitgenodigd om mee te doen aan een wetenschappelijk onderzoek naar ransomware gericht op organisaties. Dit onderzoek wordt uitgevoerd in het kader van een afstudeerscriptie van de Master Crisis and Security Management aan Leiden Universiteit.

Wat wordt er van u verwacht?
Meedoen aan het onderzoek houdt in dat u een online vragenlijst gaat invullen. De vragen hebben betrekking op de verschillende overwegingen die kunnen spelen tijdens een ransomware crisis. Het invullen van de vragenlijst kost ongeveer **15 minuten.**

Vrijwilligheid
U doet vrijwillig mee aan dit onderzoek. Daarom kunt u op elk moment tijdens het onderzoek uw deelname **stopzetten** en uw **toestemming intrekken**. U hoeft niet aan te geven waarom u stopt. U kunt tot twee weken na deelname ook uw onderzoeksgegevens in zien of laten verwijderen. Dit kunt u doen door een mail te sturen naar ransomwareonderzoek@outlook.com

Wat gebeurt er met mijn antwoorden?
De onderzoeksgegevens die we in dit onderzoek verzamelen, zullen gebruikt worden voor een afstudeerscriptie van de Master Crisis and Security Management aan de Universiteit Leiden. Uw antwoorden worden **anoniem** verwerkt en zijn voor de onderzoeker **niet** te herleiden naar identificerende metadata zoals een bepaalde datum en tijd of een IP-adres.

Het kan zo zijn dat de anonieme gegevens later beschikbaar worden gesteld voor ander wetenschappelijk onderzoek, wij volgen hier de minimale opslagtermijn van 10 jaar zoals vastgesteld in de *Nederlandse Gedragscode Wetenschapsbeoefening* van het VSNU.

De onderzoeksgegevens worden opgeslagen op beveiligde wijze volgens de richtlijnen van de Universiteit Leiden.

Heeft u vragen over het onderzoek?
Als u meer informatie over het onderzoek wilt hebben, kunt u contact opnemen met Bhaskar Dercon via ransomwareonderzoek@outlook.com

TOESTEMMING:

Door te klikken op de knop ‘Ik ga akkoord’ geeft u aan dat u:

- bovenstaande informatie heeft gelezen
- vrijwillig meedoet aan het onderzoek
- 18 jaar of ouder bent

Appendix 2: Survey questions with translation

Nr.	Dutch (question asked)	English	Possible answers
1	Gaat u akkoord met de bovengenoemde voorwaarden?	Do you agree with the stated conditions above?	Yes. (A respondent can only start the survey if they agree with the terms and conditions stated.)
2	Wat is uw geslacht?	What is your gender?	Male, female, other, prefer not to say.
3	Wat is uw leeftijd?	What is your age?	Age groups, staring 'from younger than 18' to 65+
4	Wat is uw hoogst genoten opleiding?	What is your highest completed education level?	Levels of education, ranging from primary school to a completed PhD.
5	Ik heb een adviserende rol en/of besluitvormende rol op het gebied van informatiebeveiliging.	I have an advisory and/or decision-making role in the field of information security.	Yes or no.
6	Mijn rol binnen mijn organisatie kan het best worden omschreven als:	My role within my organization is best indicated as:	Numerous roles in information security like CISO, ISO or ISM. Also options for not preferring to say or not described in option.
7	De organisatie waar ik voor werk kan worden aangeduid als:	The organization I work for can be referred to as a:	Public, private, semi-public
8	Mijn organisatie is actief in de vitale processen zoals aangeduid door de NCTV.	My organization is active in the vital processes, as indicated by the NCTV.	Yes, no, I don't know.
9	Ik ben actief voor een organisatie met tussen de:	I work for an organization with between:	Employee number groups ranging from 1-5 to more than 10.000 employees
10	Hoe lang bent u actief voor uw organisatie?	How long have you been working for your organization?	Year groups from 0-1 to more than 10 year
11	Ik volg de actualiteit rondom ransomware actief.	I actively follow the actuality around ransomware.	Linkert scale
12	Ik ben op technisch niveau bekend met de werkwijze van ransomware groepen die organisaties aanvallen.	I am technically familiar with the methods that ransomware groups use to attack organizations.	Linkert scale
13	Een uitval van systemen waardoor eindgebruikers voor een periode langer dan vier uur niet aan het werk konden, heb ik eerder ervaren binnen mijn organisatie.	I have previously experienced a failure of systems that prevented end-users from working for a period longer than four hours within my organization.	Yes, no, I prefer not to say
14	Heeft u binnen uw organisatie eerder te maken gehad met een ransomware-aanval?	Have you previously experienced a ransomware attack within your organization?	Yes: with payment, Yes: without payment, No, I prefer no to say
15	Als ik persoonlijk slachtoffer zou worden van een ransomware-aanval, zou ik in geen geval het geëiste losgeld betalen.	If I personally fell victim to a ransomware attack, I would under no circumstances pay the ransom demanded.	Linkert scale
16	Als de organisatie waarvoor ik werk slachtoffer zou worden van een ransomware-aanval, zou ik altijd	If the organization I work for would fall victim to a ransomware attack, I would always decide/advise against paying the ransom demanded.	Linkert scale

	beslissen/adviseren tegen het betalen van de eis.		
17	Een bedrijf dat losgeld betaalt als gevolg van een ransomware-aanval heeft de back-up en recovery niet goed geregeld.	An organization that pays a ransomware demand has not properly managed backup and recovery.	Linkert scale
18	Een bedrijf dat slachtoffer wordt van een succesvolle ransomware-aanval heeft dit te danken aan eigen incompetentie.	A company that falls victim to a successful ransomware attack owes its own incompetence.	Linkert scale
19	Ransomware-aanvallen houden alleen op als slachtoffers niet meer betalen.	Ransomware attacks only stop when victims stop paying.	Linkert scale
20	Het betalen van losgeld draagt bij aan het voortbestaan van criminele netwerken en is daarom onethisch.	Paying a ransom contributes to the survival of criminal networks and is therefore unethical.	Linkert scale
21	Het betalen van losgeld om een ransomware-aanval af te kopen, is niet aan te raden omdat er geen garantie is dat de criminelen daadwerkelijk een decryptiesleutel zullen verschaffen.	Paying a ransom to pay off a ransomware attack is not recommended as there is no guarantee that criminals will actually provide a decryption key.	Linkert scale
22	Als een ransomware-aanval de bedrijfscontinuïteit van een organisatie bedreigt, is het betalen van losgeld een legitieme maatregel die overwogen moet worden.	If a ransomware attack threatens an organization's business continuity, paying a ransom is a legitimate measure to consider.	Linkert scale
23	Als het geëiste losgeld bedrag lager is dan de kosten van een zelf uitgevoerde hersteloperatie, dan is het betalen van losgeld een legitieme maatregel die overwogen moet worden.	If the required ransom amount is less than the cost of a self-repair, then paying a ransom is a legitimate measure to consider.	Linkert scale
24	Het moet voor publieke of semipublieke organisaties niet mogelijk zijn om gemeenschapsgeld uit te geven aan losgeld geëist in een ransomware scenario.	It should not be possible for public or semi-public organizations to spend community money on ransom demanded in a ransomware scenario.	Linkert scale
25	In de organisatie waarvoor ik werkzaam ben, is het voorbestaan en het kunnen leveren van diensten belangrijker dan het maken van winst op de korte termijn.	In the organization I work for, long-term survival and service availability is more important than making a profit in the short term.	Linkert scale
26	Als het betalen van losgeld de aanvaller weerhoudt van het publiceren van gestolen persoonsgegevens of bedrijfsgeheimen, dan zou ik adviseren/beslissen dit te doen.	If paying a ransom prevents the attacker from disclosing stolen personal data or trade secrets, I would advise/decide to do so.	Linkert scale
27	Heeft uw organisatie volledige controle over de besluitvorming over de afwikkeling van een incident als ransomware of ligt deze autoriteit bij andere partijen?	Does your organization have full control over the decision-making process regarding an incident such as ransomware, or does this authority lie with other parties?	Completely with my organization itself, Partly with other organizations, Completely with another organization, I don’t know

28	Heeft uw organisatie crisisscenario's uitgewerkt die ingaan op de afwikkeling van een ransomware-aanval?	Has your organization developed crisis scenarios that deal with the resolution of a ransomware attack?	Yes, elaborated scenarios that have been discussed and practiced, Yes, elaborated scenarios that have not been practiced, No, no elaborated scenarios, but an ambition to develop them, No, no elaborated scenarios and no ambition to develop them, I don't know
29	Als een ransomware-aanval het voorbestaan van een organisatie bedreigt, zou ik adviseren om over te gaan tot betaling.	If a ransomware attack threatens the survival of an organization, I would recommend making the ransom payment.	
30	Als het geëiste losgeld bedrag lager is dan de kosten voor een zelfstandig uitgevoerde hersteloperatie, zou ik adviseren om over te gaan tot betaling.	If the required ransom amount is less than the cost for an independently performed repair operation, I would advise the organization to pay.	Linkert scale
31	Het hebben van een verzekering die de kosten van losgeld dekt, zou het afkopen van een ransomware-aanval voor mijn organisatie aannemelijker maken.	Having insurance that covers ransom costs would make it more plausible to pay off a ransomware attack for my organization.	Linkert scale
32	Als er binnen mijn organisatie gekozen wordt om over te gaan tot betaling van de gijzelnemers, zou ik adviseren/proberen te onderhandelen over de prijs.	If my organization chooses to pay the hostage-takers, I would advise/try to negotiate the price.	Linkert scale
33	Binnen de organisatie waarvoor ik werk wordt open gecommuniceerd over risico's en dreigingen op het gebied van cybersecurity.	Within the organization for which I work, there is open communication about risks and threats regarding cybersecurity.	Linkert scale
34	Als ik waarschuw voor een bepaalde cybersecurity dreiging binnen mijn organisatie zal dit voldoende serieus genomen worden en zullen er maatregelen genomen worden, ook als dit investeringen vereist.	If I warn about a certain cybersecurity threat within my organization, this will be taken seriously, and measures will be taken, even if this requires investments.	Linkert scale
35	Binnen mijn organisatie zijn eerder cybersecurity risico's voor lief genomen of genegeerd. Ook als hier expliciet voor gewaarschuwd was.	Within my organization, cybersecurity risks have previously been taken for granted or ignored, even if there were explicit warnings.	Linkert scale
36	Het advies van de politie om nooit losgeld te betalen aan ransomware-actoren is belangrijk in mijn overweging hierover.	The advice from the police to never pay a ransom to ransomware actors is important in my consideration of this.	Linkert scale
37	Omdat de overheid tegen het betalen van ransomware actoren adviseert, zal ik altijd adviseren/beslissen om niet	Because the government advises against paying ransomware actors, I	Linkert scale

	over te gaan tot het betalen van het geëiste losgeld.	will always advise/decide not to pay the ransom demanded.	
38	In mijn overweging om wel of niet te betalen zou het welzijn van mijn klanten en behoud van hun vertrouwen in mijn organisatie belangrijk zijn.	In my consideration of whether or not to pay, the well-being of my customers and maintaining their confidence in my organization will be important.	Linkert scale
39	In mijn overweging om wel of niet te betalen zou het welzijn van mijn ketenpartners en behoud van hun vertrouwen in mijn organisatie belangrijk zijn.	In my consideration of whether or not to pay, the well-being of my chain partners and maintaining their confidence in my organization would be important.	Linkert scale
40	Als mijn organisatie het slachtoffer wordt van een ransomware-aanval, zou ik adviseren om te proberen dit uit de media houden.	If my organization falls victim to a ransomware attack, I would advise trying to keep it out of the media.	Linkert scale
41	Als mijn organisatie het slachtoffer wordt van een ransomware-aanval, zou ik adviseren/beslissen om zo veel mogelijk transparant te zijn naar buitenwereld.	If my organization falls victim to a ransomware attack, I would advise/decide to be as transparant as possible to the outside world.	Linkert scale

100 point scale model

Nr.	Factor	Translation
1	Het voorkomen van langdurige stilstand van bedrijfsprocessen	Preventing long-term stoppages of business processes
2	De kosten van het zelf herstellen van systemen tegenover het betalen van het losgeld	The cost of an independently performed repair operation in relation to paying ransom
3	Het verliezen van cruciale data	Losing crucial data
4	De hoogte van het geëiste losgeld bedrag	The amount of demanded ransom
5	Het advies van de politie om nooit losgeld te betalen	The advice from the police to never pay a ransom
6	Het niet willen bijdragen aan een crimineel verdienmodel	Not wanting to contribute to a criminal revenue model
7	De onzekerheid of de betaling ook daadwerkelijk tot decryptie leidt	The uncertainty whether the payment actually leads to decryption
8	De belangen van klanten en ketenpartners	The interests of customers and chain partners
9	Het oplopen van reputatieschade	Taking reputational damage

43	Als het geëiste losgeld hoger is dan ... procent van de maandomzet (voor publieke organisaties, lees: budget per maand) dan zou ik adviseren/besluiten om niet te betalen. Ter illustratie: afhankelijk van de grote van een organisatie ligt de eis meestal tussen de 50 duizend en 10 miljoen euro.	If the ransom demanded is higher than ... percent of the monthly turnover (for public organizations, read: budget per month) then I would advise / decide not to pay. To illustrate: depending on the size of an organization, the requirement is usually between 50 thousand and 10 million euros.	Slider 0 tot 100 percent

	Als dit geen invloed op uw beslissingsproces heeft of u hier geen inschatting van kan maken, laat de schuifregelaar dan op 0% staan.	If this does not affect your decision-making process or if you cannot estimate it, leave the slider at 0%.	
44	Als het geëiste losgeld meer dan .... euro is, zou ik adviseren/beslissen het betalen van het losgeld sowieso niet in overweging nemen.	If the ransom demanded is more than ... euros, I would advise/decide to not consider paying the ransom.	Numerous options ranging from 10.000 euro to 7,5 million euro. Also the option that it does not influence the decision making.
45	Als de bedrijfsprocessen van mijn organisatie stil komen te liggen door een ransomware-aanval, schat ik dat dit ongeveer ..... euro per dag kost. Als u hier geen schatting van kunt of wilt maken reageer dan: -1	If the business processes of my organization come to a standstill by a ransomware attack, I estimate that this is about ..... euros a day costs. If you cannot or do not want to estimate this, please respond: -1	The respondent can put in an amount in euro.
46	Als het ondernemen van een zelfstandige hersteloperatie langer dan ... zou kosten, en mijn organisatie die dagen dus minimale diensten of producten kan leveren, zou ik adviseren over te gaan tot het betalen van losgeld.	If undertaking an independent repair operation would take longer than ... days, and my organization could only provide minimal services or products during those days, I would advise/decide to pay ransom.	Range from 1 day to longer than a month. Also the option that it does not influence the decision making.

Appendix 3: T-test sectorial comparison

Group Statistics: notable differences vital/non-vital sector

	Vital/Non-vital	N	Mean	Std. Deviation	Std. Error Mean
Losing crucial data	Vital	26	83.6538	15.44783	3.02957
	Non-vital	25	90.1200	12.50773	2.50155
Preventing long-term stoppages of business processes	Vital	26	81.2308	13.95509	2.73682
	Non-vital	25	88.9200	11.25803	2.25161
Taking reputational damage	Yes	26	61.6538	28.18360	5.52726
	Non-vital	25	68.9600	27.86647	5.57329
The amount of demanded ransom	Yes	26	32.5769	24.91774	4.88677
	Non-vital	25	46.8800	31.01924	6.20385

Independent Samples Test: Vital and non-vital organizations

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Losing crucial data	Equal variances assumed	.521	.474	-1.639	49	.108	-6.46615	3.94526	-14.39444	1.46214
	Equal variances not assumed			-1.646	47.642	.106	-6.46615	3.92887	-14.36721	1.43490
Preventing long-term stoppages of business processes	Equal variances assumed	.109	.742	-2.160	49	.036	-7.68923	3.55903	-14.84136	-.53710
	Equal variances not assumed			-2.170	47.587	.035	-7.68923	3.54400	-14.81651	-.56195
Taking reputational damage	Equal variances assumed	.082	.775	-.931	49	.357	-7.30615	7.85112	-23.08357	8.47126
	Equal variances not assumed			-.931	48.960	.357	-7.30615	7.84934	-23.08033	8.46802
The amount of demanded ransom	Equal variances assumed	1.340	.253	-1.819	49	.075	-14.30308	7.86336	-30.10510	1.49894
	Equal variances not assumed			-1.811	46.016	.077	-14.30308	7.89736	-30.19949	1.59334

Group Statistics

	Public/Private	N	Mean	Std. Deviation	Std. Error Mean
The uncertainty whether the payment actually leads to decryption	Public organization	21	62.5714	30.49684	6.65496
	Private organization	36	50.9167	26.45252	4.40875
The advice from the police to never pay a ransom	Public organization	21	42.1429	33.88109	7.39346
	Private organization	36	30.5000	29.91846	4.98641

Independent Samples Test: Public and private organizations

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
The uncertainty whether the payment actually leads to decryption	Equal variances assumed	1.557	.217	1.516	55	.135	11.65476	7.68587	-3.74806	27.05759
	Equal variances not assumed			1.460	37.302	.153	11.65476	7.98283	-4.51557	27.82509
The advice from the police to never pay a ransom	Equal variances assumed	.466	.498	1.350	55	.183	11.64286	8.62671	-5.64546	28.93118
	Equal variances not assumed			1.306	37.857	.200	11.64286	8.91782	-6.41257	29.69829

Appendix 4: Targeted ransomware decision tree