The role of High Reliability Organization (HRO) theory in cyber security

A case study of the cyber security in a hospital from a HRO perspective

Name:	Bart Snijdelaar
Student Number:	S1483722
Supervisor:	Dr. Jaap Reijling
2nd reader:	Dr. ir. Vlad Niculescu-Dinca
Assignment:	Master thesis Crisis and Security Management
Date:	02-06-2020

Table of contents

Abstract

The research question of this thesis is: *To what extent have the ideas derived from High Reliability Organizations been incorporated in an organization concerned with cyber security, and how can discrepancies be explained?* After creating of a theoretical frame work, a case study design (consisting of document analysis and interviews) was used to find an answer to the research question. The five principles of HRO theory were operationalized to allow researching cyber security. From a theoretical perspective, the five principles of HRO theory can be used in research on cyber security. To 'test' this in practice a case study was done in a hospital. It was found that none of the HRO principles have been fully incorporated in the hospital's approach to cyber security. The failure to prioritize cyber security in the hospital and the low level of awareness among employees are the two main explanations for this finding. Applying the principles of HRO theory to cyber security might allow a better understanding of the requirements needed to establish highly reliable cyber security. The case study in this study showed that barriers need to be overcome to be able to fully implement the principles of HRO theory in an organization which primary goals is not safety or reliability. This thesis has identified what these barriers are and has improved our understanding on how HRO theory can improve cyber security.

Acknowledgements

The research and writing process of this thesis has certainly not been without hiccups. Without the help and cooperation of number of people writing this thesis would not have been possible.

I would first like to thank my thesis advisor Dr. Jaap Reijling of the Faculty Governance and Global Affairs at Leiden University. He consistently allowed this paper to be my own work, but steered me in the right direction whenever he thought I needed it. I would also like to acknowledge Dr. ir. Vlad Niculescu-Dinca of the Institute for Security and Global Affairs at Leiden Uiversity for being the second reader of this thesis.

Second, I want to thank the three interviewees of the hospital. Without their willingness and help, it would not have been possible to do the case study. Their cooperation was vital. Therefore, I want to thank them for their openness and for taking the time for me to interview them.

Finally, I must express my very profound gratitude to my parents for providing me with support and encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Love you! I want to especially thank my father for helping me structuring and rewriting this thesis. Dad, without your help, it would have taken much longer to finish up this thesis. Thank you!

Chapter 1: Introduction

Our society increasingly relies on digital systems and processes and this has changed how society functions. In fact, society has become so reliant on the 'digital' that it does not function anymore without it. While the benefits of this transformation are often celebrated, a new set of challenges have also arisen. One of these new challenges is how to secure digital systems and processes (NCTV, 2019, p. 11); this is what we call cyber security. Efforts to improve cyber security are challenging for several reasons. First, digital processes and systems are growing, both in size and complexity. This means there is more to secure and it becomes more and more difficult to do this. The growth in digital processes and systems also results in a larger attack surface. So, malicious actors have a large number of 'entrance' through which they can gain unauthorized access. Second, many organizations have failed so far to implement even basic security measures which leaves them vulnerable to cyber-attacks. Third, due to the rise of cyber-crime-as-a-service, even layman can now simply order a cyber-attack online. This greatly increases the threat levels (NCTV, 2019, p. 12). In short, securing our digital processes and systems is a big challenge. Digital systems and processes must be secured and reliable. Nowadays, having good cyber security is essential for a stable and functioning society.

This thesis aims to better understand cyber security by analysing it from the perspective of the High Reliability Organization (HRO) theory. High Reliability Organizations (HROs) are organizations operating in complex, technical and hazardous environments. Unattended errors in these organizations could lead to large-scale crises. Therefore, there is limited room for error. Errors that do occur need to be swiftly and adequately addressed. HROs have created systems and methods that limit the amount and the impact of errors; this has made HROs extraordinarily reliable (Rochlin, 1996). The principles of HRO theory, on which these systems and methods are based, form the basis of this thesis. 'Translating' these principles to cyber security might allow a better understanding of the requirements needed to establish highly reliable cyber security. This 'translating' of HRO theory to cyber security, and testing of this 'translation' in a case study, is the subject of this thesis. The research question of this thesis therefore is: *To what extent have the ideas derived from High Reliability Organizations been incorporated in an organization concerned with cyber security, and how can discrepancies be explained?*

Originally, HRO theory was first researched in specific organizations such as the control room of nuclear power plants (Schulman, 1993) and the flight decks of aircraft carriers (Weick & Roberts, 1993). Since then HRO theory has been applied to other fields. Examples are the

medical (Robert, Madsen, Desai, & Van Stralen, 2005), the military (Zohar & Luria, 2003) and the aviation sector (Shawn Burke, Wilson, & Salas, 2005). HRO theory has also been applied to cyber security. However, this was either for quantitative research (Burns, 2019), or applied to organizations that already had (cyber) security as one of their top priorities, such as the US Defense Department (Winnefeld Jr., Kirchhoff, & Upton, 2015). This thesis concerns qualitative research of a non-cyber security focused organization: a hospital. Although, in general, hospitals are less cyber security focused compared with an US Defense Department, failing cyber security in hospitals can also cause significant harm.

To first answer the question if, from a theoretical perspective, the principles of HRO theory can be applied to cyber security, a theoretical framework is created (chapter 2). This chapter consists of three sections: a section on cyber security, a section on HRO theory and a section on if, and how, the principles of HRO theory can be 'translated' to cyber security. The next chapter is the methodology chapter (chapter 3). In this chapter, the research design is explained. This includes the research method, data collection and data analysis. This is followed by a discussion on how the HRO theory can be operationalized to allow researching cyber security. To provide an answer to the research question an in-depth case study is presented in chapter 4. The case study is an analysis of cyber security in a Dutch hospital. The name and location of this hospital cannot be revealed. The hospital has requested anonymity because of the sensitivity of the information that was provided for this research. In this chapter it is analysed to what extent the principles of HRO theory are incorporated in the hospital's approach to cyber security. In chapter 5 conclusions are drawn and recommendations are formulated.

Chapter 2: Theoretical Framework

This chapter discusses if, from a theoretical perspective, it is possible to incorporate the principles of HRO theory into cyber security. In the first section (2.1), the National Institute of Standards and Technology (NIST) framework for Improving Critical Infrastructure Cyber Security is introduced to help understand the process of cyber security and to define cyber security as used in this thesis. In the second section (2.2), HRO theory is discussed. It sets out what the HRO theory entails and discusses the main criticism on this theory. In the third section (2.3), the principles of HRO theory are conceptualized and is discussed if, and how, the functions of the NIST framework core can be applied to the principles of the HRO theory.

2.1 Cyber Security

There is no agreed definition of cyber security in academics. Multiple publications have tried to come with one definition of cyber security (Craigen, Diakun-Thibault, & Purse, 2014; Schatz, Bashroush, & Wall, 2017), but so far these have not been widely adopted. Each organization, academic and expert uses his/her/its own definition. Thus it must be established what definition for cyber security is used in this thesis. This thesis uses the NIST framework to define cyber security (Barrett, 2018). In the following section, the NIST framework is introduced and it is explained why this particular framework has been selected.

2.1.1 NIST framework for Improving Critical Infrastructure Cyber Security

The NIST framework for Improving Critical Infrastructure Cyber Security has been created in consultation with both public and private stakeholders. This framework contains of a core which presents key cyber security outcomes which are helpful in managing cyber security risks. The core includes five functions which aid an organization in expressing its management of cyber security (Barrett, 2018);

1. Identify: NIST defines the objective of the identify function as to '*Develop an organizational understanding to manage cyber security risk to systems, people, assets, data, and capabilities*' (Barrett, 2018, p. 7). The identify function highlights the importance of having a good understanding of an organization. It must be clear what the strengths and weaknesses are of an organization. Furthermore, an understanding of the outside world is also essential in determining what the main risks are.
2. Protect: NIST defines the objective of the protect function as to '*Develop and implement appropriate safeguards to ensure delivery of critical services*' (Barrett, 2018, p. 7). This function includes the prevention of cyber-attacks. Sufficient security measures are

required to protect a system against external attacks. The impact of these attacks can be limited and contained to a certain extent.

3. Detect: NIST defines the objective of the detect function as to '*Develop and implement appropriate activities to identify the occurrence of a cyber security event*' (Barrett, 2018, p. 7). This function is straightforward and focuses on techniques to detect cyber incidents.
4. Respond: NIST defines the objective of the respond function as to '*Develop and implement appropriate activities to take action regarding a detected cyber security incident*' (Barrett, 2018, p. 8). When a cyber-attack has been successful, active measures have to be taken to contain and counter the threat. The strategies and techniques used to actively contain and counter an attack fall under this function.
5. Recover: NIST defines the objective of the Recover function as to '*Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security incident'* (Barrett, 2018, p. 8). After a cyber incident has happened, there is a need for recovery. Also, an evaluation of the cyber incident is required to further strengthen cyber security.

The NIST framework core helps in understanding the process of cyber security. Each of the five functions are important steps in the cyber security process. From this, the definition of cyber security, as used in this thesis, can be derived. This definition is as follow: '*Cyber security is the continuous process of securing digital processes and systems against cyber-attacks by identifying risks, protecting against cyber-attacks, detecting cyber-attacks, responding to cyber-attacks and recovering from cyber-attacks*'. This definition sees cyber security as a continuous process. New threats and issues can arise quickly. Organizations must constantly adapt to these new threats and issues; it is a never ending process. Not only is the importance of prevention of cyber-attacks included in the definition, but it also emphasizes the importance of the response to, and recovery from, a cyber-attack. These are all essential functions, because it is not a question of 'if' a cyber incident will happen but 'when' it will happen.

An important note is that this thesis is mainly covering the aspects of the risks of cyber-attacks and the damage these attacks are causing. While acknowledging that also malfunctioning and outages of digital systems and processes can cause severe damage, discussion on preventing of, and responding to, these risks are outside the scope of the thesis.

2.1.2 Conclusion

This thesis defines cyber security as a continuous process. Organizations must continuously identify risks and detect cyber incidents. Constant protection against cyber threats is necessary for ensuring good cyber security. The NIST framework core identifies five functions that are needed to secure digital systems and processes. Each of the functions must be accounted for in the design of reliable cyber security systems.

2.2 High Reliability Organizations

Failure is normal in most organizations. While most organizations aim for a 'zero failure rate', they realise that this is an unrealistic goal. Rather, they appreciate the learning value a failure can have. These organizations have adopted a 'trial-by-error' approach to learning (LaPorte & Consolini, 1991, pp. 25-26). This approach is known as incrementalism, in which it is assumed that not all errors can be avoided and that errors are valued as a learning experience. A key assumption of incrementalism is that these errors are '*limited and the consequences are bearable or reversible, with the costs less than the value of the improvements learned from the feedback analysis*' (LaPorte & Consolini, 1991, p. 27). However, for some organizations the consequences of errors are not bearable or reversible. In these organizations even minor errors can escalate into major crises, causing severe damage and even fatalities. Thus, in these organizations errors must be avoided at all costs (LaPorte & Consolini, 1991, pp. 27-29). Such organizations are known as High Reliability Organizations (HROs). HROs operate complex technical systems at an extremely high level of reliability, both during 'normal' circumstances and also during peak moments when the organization is under high pressure. HROs have to be capable to overcome these peak moments and remain reliable at all times. In other words, the number and impact of errors that can be 'allowed' is limited to an absolute minimum (La Porte, 1996). Since the level of performance and reliability of these organizations is very high, understanding how they do establish this can be of great value for science and for society. Example of HROs that were studied extensively are aircraft carriers (Weick & Roberts, 1993) and nuclear power plants (Schulman, 1993).

The theory of HROs contradicts the work of Charles Perrow, which is one of the foundational works on failure and errors. Perrow (1984) argues that it is not possible to prevent all failures from escalating into a crisis. This is especially true when systems and organizations are tightly coupled and very complex. As a consequence only a limited number of the staff of such an organization can fully grasp the design of the whole system. Hence, a trivial error can go unnoticed and develop into a large-scale crisis. The tightly coupled systems cause the effects

of errors to spread quickly over an organization. Perrow sees the escalation of an error as a 'normal accident'. They are normal, because these accidents cannot be prevented (Perrow, 1984). However, HRO theory states that escalation can be prevented by early detection and reaction. For this it is important to create a state of mindfulness in organizations (Weick & Sutcliffe, 2007). This state of mindfulness allows an organization to limit the effects of errors and increase reliability. Weick and Sutcliffe have identified five organizing principles that create the needed state of mindfulness. These organizing principles are:

1. Preoccupation with failure: Small failures and errors are not ignored by HROs. They carefully analyse every small failure and error to assure that this is not a warning for a larger failure or error. In HROs, there is a culture in which it is safe to report errors and mistakes. It is actually rewarded when an individual reports his or her own error. Furthermore, close-calls are not regarded as a success, because in the end there was no damage, but as a situation in which it almost went wrong. 'How it almost went wrong' is always carefully analysed in order to improve the organization (Weick & Sutcliffe, 2007, pp. 54-59).
2. Reluctance to simplify interpretations: HROs work with complex systems. Simplification would help in understanding these systems. However, this could also result in disregarding certain dangerous aspects of these systems. HROs can, and do not, rely on the simple interpretation of a system, but instead focus on details and respect the complexity. Individuals working in HRO are constantly challenging other people's interpretation. This results in diverse perspectives on the same problem, which improves the understanding of the scope of the problem. This constant challenging of each other is only possible in a culture in which trust and credibility are high and valued. Having a diverse group of people is essential for understanding all aspects of a problem. Such a group is more able to adapt to unexpected and changing circumstances (Weick & Sutcliffe, 2007, pp. 59-62).
3. Sensitivity to operations: In HROs, the most important layer of the organization is not the management layer, but the 'boots on the ground'. Who has authority is decided by expertise, not by rank. This means that, in certain circumstances, the lower-level technicians have more authority in an HRO than the managers. A choice is made to focus on the short-term performance of the organization instead of long-term strategy. This focus on the short-term performance of the organization, makes it possible to spot any anomalies. There is a high degree of situational awareness. Furthermore, everyone

in the organization is provided with real-time updates, not just the managers. Hence, more people have a good understanding of what is going on. Constant communication between different groups of an organization is needed to enhance trust and credibility, and to understand the complex system better by being exposed to the interpretation of other departments (Weick & Sutcliffe, 2007, pp. 62-65).

4. Commitment to resilience: It is impossible to prevent all errors. Some errors slip through the mazes of the prevention net. When these errors escalate into a crisis, organizations must react to this. It is often assumed that anticipation is the best way to prepare for a crisis. While the focus on anticipation prepares an organization for certain crises, most crises are unexpected and unknown beforehand and cannot be anticipated. When an extensive anticipative plan has been created, a certain narrowmindedness makes the organization ignore crises that have not been accounted for in their plans. Furthermore, it gives people the illusion that everything is under control, even though this might not be true. Since many threats are unknown and cannot be prepared for, this focus on anticipations stifles the development of skills such as improvisation, resilience and intelligent reaction. The idea of resilience is that problems are unknown and unexpected. There is no information available beforehand. People start countering the error even though they do not have full information. It is necessary to act while thinking. HROs assume that they will be surprised. They do not anticipate known errors, but value the skills necessary to react to unknowns. HROs develop these resilience skills by testing their organization. From these tests, lessons are learned on how to better mitigate problems when they occur (Weick & Sutcliffe, 2007, pp. 67-73).
5. Deference to expertise: in normal circumstances, (non-)HROs work within a hierarchy in which the higher-ranked make the decisions that are carried out by the lower-ranked. In non-HROs, this same hierarchy is used in times of crisis. This means that the higher-ranked always make the important decisions; in non-HROs rank goes above expertise. In HROs, the person that makes the important decisions differs per situation. Who that person is depends on the expertise that that person has on the issue at hand. So, in HROs, the hierarchy changes depending on the circumstances and expertise is valued over rank. Since in HROs decisions have to be made quickly, the persons that know most about the systems (usually the operators) are best suited to make these decisions. In HROs, it is valued when people know the limits of their knowledge and ask for help when they do not understand. This type of culture makes an organizations more reliable (Weick & Sutcliffe, 2007, pp. 73-77).

In HRO theory it is not argued that all errors can be prevented. This is simply impossible. However, swift detection and reaction to these errors is possible. The first three organizing principles from Weick & Sutcliffe focus on the early detection of errors and the prevention of escalation. Without an adequate reaction to these errors, these can escalate into a large crisis. The last two organizing principles describe what HROs do when errors have gone unnoticed and grown more dangerous. They also describe how a crisis, as a result of escalated errors, can be contained, limited and how to return to normal (Weick & Sutcliffe, 2007, p. 83).

2.2.1 Criticism on HRO theory

HRO theory has not been free of criticism. The main criticism comes from Levenson et al. (2009). They argue that HRO theory fails to make a distinction between safety and reliability. In HRO theory, it is assumed that if a system works reliable and secure it is also safe, because there are no accidents. Levenson et al. state that an organization can be safe but not reliable; or not safe, but reliable. For example, a chemical plant that produces toxic chemicals could be reliable, because it continuously produces chemicals; but is not safe, because it pollutes the environment (Levenson, Dulac, Marais, & Carroll, 2009, pp. 234-236). For this thesis, the distinction between reliability and safety is irrelevant. First, this thesis focuses on deliberate cyber-attacks, which is a security issue, and not on malfunctioning and outages, which are safety issues. Second, for the cyberspace, a system is no longer reliable, when security has been breached. By having had some form of unauthorized access to a system, interference can happen at any moment. So, even if a system still fully functions, the fact that security has been breached, makes a system unreliable.

Another point of critique from Leveson et al. (2009, pp. 236-237) focuses on the decentralized decision-making of HRO theory. They question the HRO principle that in certain circumstances lower ranked operators are more able to make decisions than higher ranked managers. There are many examples in which operators made decisions that turned out to be bad. While in some cases the HRO principle might be valid, allowing operators to make decisions does not always directly result in better decision-making. Levenson et al. argues that operators cannot always oversee the effects of their decisions. A decision that helps in one area, might do damage in another area (so-called ‘waterbed effect’). Hence, Levenson et al. doubt the effectiveness of decentralizing the decision-making. However, HRO theory argues that only in situations of high stress on an organization, deference to expertise is necessary. In ‘normal’ circumstances, there is also a ‘normal’ hierarchy (Weick & Sutcliffe, 2007, p. 17). Furthermore, HRO theory does not argue that the expert approach is perfect. Actually, it is emphasized that in time-pressured

and high stress situations, getting all the necessary information is difficult. Hence, the experts must respond without having full and accurate information; they then have to quickly learn from errors through fast feedback (Weick & Sutcliffe, 2007, p. 69). Thus, error does occur in HROs during moments of high stress. What differentiates HROs from non-HRO organizations is the way they react to errors.

Lastly, Levenson et al. (2009, pp. 237-241) criticize the generalizability of the case studies that form the basis of HRO theory. They argue that most of the case studies have been of organizations of which one of their primary goals is safety or reliability. Most organizations have other goals as well, such as profit-making. These different goals might clash. Hence, HRO theory might be more difficult to implement in other organizations. To demonstrate this Levenson et al. point to the technology used by HROs. HROs often use older technology that have proved to be safe and reliable. However, this technology might not be the most efficient. Non-HROs might be pressured to implement new technologies that are more efficient. The pressure prevents employees from gaining a good understanding of these new technologies which makes them less safe and reliable. So, non-HROs have other priorities than HROs, which makes implementing ideas derived from HROs challenging.

2.2.2 Conclusion

In this section, HRO theory has been introduced, including the five organizing principles that make an organization highly reliable: preoccupation with failure, reluctance to simplify, sensitivity to operations, commitment to resilience and deference to expertise. Also, several points of criticism on HRO, have been addressed. In the next section, the five organizing principles of HRO are translated to the functions NIST conceptualized to cyber security.

2.3 Conceptualization of the principles of HRO theory to cyber security

In this section the principles of HRO theory are ‘translated’ or conceptualized to cyber security. The object is to answer the question if, from a theoretical perspective, HRO theory can be applied to cyber security. To answer this question the five principles are conceptualized. The purpose of conceptualization is to refine and specify what is meant whit each of the five the principles of HRO theory. Conceptualization is the first step in making the principles of HRO theory measurable. In the following, it is discussed how the principles of HRO theory are ‘connected’ with the functions of the NIST framework core. Or, in other words, are the functions of the NIST framework core applicable to the principles of the HRO theory?

2.3.1 Preoccupation with failure

Failures are common in cyber security. These are often the result of vulnerabilities which by The European Union Agency for Cyber Security are defined as '*the existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.*' (ENISA 1, sd). Hence, vulnerabilities can be the result of insufficient security measures or a lack of security. Since there is a high degree of innovation and development in the cyber world, new vulnerabilities can arise quickly, as well as methods to exploit these. Vulnerabilities involve any weakness that can negatively affect a system or network (NIST, 2012, pp. 9-10). These vulnerabilities can be used by an unauthorized third party to gain access to a system. Due to their actions, systems can fail or can perform unusually or unexpectedly. The duration from the moment that an intruder gained access, until the moment of detection is known as dwell time. In 2018, the median dwell time was 78 days (Fire Eye, 2019). The possible damage that can be done during such a long time span can be immense. This shows that one needs to be preoccupied with failure by **identifying** vulnerabilities and **detecting** irregularities in systems. Early identification and detection allows for a quick, adequate and timely response. So, this principle of 'preoccupation with failure' can be further specified as 'the preoccupation with failure to identify vulnerabilities and detect irregularities or anomalies'.

Preoccupation with failure				
The preoccupation with failure to identify vulnerabilities and detect irregularities or anomalies				
Identify	**Protect**	**Detect**	**Respond**	**Recover**
x		x		

2.3.2 Reluctance to simplify interpretations

'Reluctance to simplify interpretations' means that nothing is taking for granted. Employees from HRO's are constantly being challenged to assure that they keep an open mind. An effort is made to prevent tunnel vision and confirmation biases. Every anomaly that is unusual must be carefully analysed to exclude the possibility of evolving to a major incident.

There is a high pace of innovation in the cyber world. While new technologies and developments have advantages, they also come with new risks. The high pace of innovation is not limited to the 'good guys'. Malicious actors also develop new techniques and methods to breach security. These new methods and techniques are often very creative and innovative. An

example of this are the so-called zero-day exploits. These are vulnerabilities that are unknown to not only the user, but also the vendor, of software. Hence the name, the vendor has known this exploit for zero days. Such an exploit often provides a backdoor into a network. One of the few ways to detect such an intrusion is by carefully analysing any anomalies that are caused by the intruder (ENISA 2, sd). The IT staff responsible for cyber security much be as innovative and creative as the malicious actors. This innovative and creative mind-set requires a critical approach to the status quo of cyber security with no room for simplifications of any incidents. Only with this mind-set, it is possible to keep up with cyber criminals. Any anomaly must be carefully analysed to **identify** new cyber threats and **detect** cyber-attacks. The only way to keep up with the high pace of innovation and creativity among cyber-attackers, constant challenging of an organization's methods and assumptions is needed.

Reluctance to simplify interpretations				
High pace of innovation and creativity among cyber-attackers. Only way to keep up is the constant challenging of an organization's methods and assumptions.				
Identify	**Protect**	**Detect**	**Respond**	**Recover**
x		x		

2.3.3 Sensitivity to operations

For this thesis, it is assumed that cyber security is part of every organizations' 'operations'. Many organizations do not function without their digital systems and processes. While it is acknowledged that cyber security is often not the main priority for most organizations, a good cyber security system is essential for the continuation and stability of an organization.

For an organization, having a clear picture of all possible cyber threats is important. By answering questions as 'Who and what forms the main threat? What methods do they use?' an organization is better suited to protect itself against cyber-attacks. This gathering of information of the main threats is what is meant with threat intelligence. Since cyberspace is immense, an organization can never independently gather sufficient threat intelligence. Therefore, cooperation between different organizations is essential. Sharing threat intelligence greatly helps in understanding and countering threats (Metz, 2017).

In organizations cyber security is often seen as only the responsibility of the cyber security team or IT department. Non-IT departments are often not involved when it comes to cyber security issues. However, it is essential that all employees understand the main risks. Cyber security is

as strong as its weakest link. If one of the employees is not committed to cyber security, cyber security is immediately significantly weakened. Cyber security is the responsibility of the whole organization (KPMG, 2013, pp. 10-11). People are often unaware of the risks of modern technology and the dark side of our global connectedness. Therefore, people are often the weakest link in cyber security (Kapersky, n.d.).

In a perfect world, all employees of an organization will have a full understanding of cyber security. However, this is unrealistic and the required level of awareness also differs per role. The NIST states that '*Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly'* (Wilson & Hash, 2003, pp. 8-9). Most cyber-attacks use relatively simple methods, but are successful since basic awareness is lacking (NCTV, 2019, p. 18). An example of this is phishing. Malicious actors pretend to be a trustworthy actor by faking their identity. With this fake identity, they lure their target into sharing sensitive information, such as passwords. Phishing often involves fake emails that pretend to originate form a trusted source. Opening a link or a file in this email, provides a malicious actor access to a network (NCTV, 2019, p. 34). Improving awareness among employees about common cyber-attack methods and techniques, such as phishing, strengthens cyber security. All employees must be able to **identify** and **detect** common cyber-attacks, to **protect** themselves (and the organization) against these, and to **respond** to cyber incidents. In short, organizations need to have a clear picture of the main cyber threats to their organization. Moreover, all employees need to be aware about common threats and cyber-attacks. High cyber security awareness improves the overall cyber security. A good understanding of cyber threats and risks, improves an organizations ability to prevent and react to these threats and risks. This improves the likelihood of early identification and detection. Furthermore, a good understanding aids in the process of **protecting** and **responding** to these threats and risks.

Sensitivity to operations				
There has to be sharing of threat intelligence and all employees need a minimal level of cyber security awareness				
Identify	**Protect**	**Detect**	**Respond**	**Recover**
x	x	x	x	

2.3.4 Commitment to resilience

As discussed in the previous sections cyber security and cyber threats are subject to continuous and highly sophisticated innovation. New threats can arise at any moment. It is impossible to anticipate all of these new innovations. De Crespigny (2012, p. 7) emphasizes this problem by quoting Donald Rumsfeld. Even though this quote is not about cyber security, it does illustrate one of the main challenges of cyber security: *'There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know.'* (Rumsfeld, 2002).

Many threats and vulnerabilities are unknown at this moment (NIST, 2012, pp. 9-10). Since a threat is unknown, it cannot be anticipated upon. It is during a cyber-attack that the unknown threats becomes known. In this occasion an organization has to react without having all the information which implies improvisation and acting while thinking. During such an attack the organization needs to be cyber resilient; it is the ability to deliver the intended outcome despite adverse cyber-attacks. Ross et al. (2019, pp. 80-82) identify several cyber resilience objectives. These help in understanding different phases of cyber resilience. First, when hit by a cyber-attack, an organization must continue functioning, albeit at a lower efficiency. In order to continue operations, an organization needs to have reserve resources that can be allocated to replace damaged systems (Batteau, 2011, p. 40). Second, at the same time, an organization must contain the impact of the attack. Limiting the damage is key. Beforehand, an organization should have identified what its 'crown jewels' are. These are the main assets that are most valuable to an organization. During a cyber incident, protecting these 'crown jewels' should have priority. Third, when the cyber-attack is under control, reconstitution starts. This is a process in which damaged and infected systems are restored to their normal functionality. Either systems are replaced or the damage is repaired. A risk with repairing is that when systems have not been thoroughly wiped, an unauthorized third party continues to have presence on a system. For reconstitution, it is beneficial when regular back-ups had been made in the past. As Schofield (2008) already stated 'data doesn't really exist unless you have two copies of it. Preferably more'. This allows the system to be restored to its most recent state before the cyber-attack (Ross, Pillitteri, Graubart, Bodeau, & McQuaid, 2019, pp. 80-82). Fourth, it is necessary to understand how the cyber-attack could happen. The cyber-attack and the response need to be evaluated. What are the lessons learned? Fifth is implementing the lessons learned to strengthen cyber security. Thus, the cyber security of an organization is transformed and re-architected to

prevent future attacks and improve the response to successful attacks (Ross, Pillitteri, Graubart, Bodeau, & McQuaid, 2019, pp. 80-82).

Organizations must have the ability to mitigate cyber-attacks. HRO theory sees resilience as mitigation and not anticipation. While some degree of anticipation is positive, an overreliance on anticipation prevents HROs to respond to the unknown. Hence, HRO prefer mitigation over anticipation (Weick & Sutcliffe, 2007, pp. 67-73). This mind-set also applies to the cyberspace. Obviously cyber security experts need to have broad understanding of cyber security, but also skills to quickly **respond** to and **recover** from cyber incidents. Since not all cyber-attacks can be anticipated, skills such as real-time learning, improvisation and creativity are highly valued. Developing these skills requires regular training and testing. This allows cyber security professionals to help each other out in times of need (Weick & Sutcliffe, 2007, p. 78).

Commitment to resilience				
Cyber resilience is the ability to respond to and recover from breaches in cyber security caused by cyber-attacks.				
Identify	**Protect**	**Detect**	**Respond**	**Recover**
			x	x

2.3.5 Deference to expertise

Weick and Sutcliffe (2007, pp. 73-77) argue that in times of high stress on an organization, as caused by an major cyber-attack, ‘deference to expertise’ is necessary. The normal hierarchy is suspended and instead a structure in which the experts take command is created. The experts are given considerable leeway to make their own decisions without consulting higher ranking managers and executives. They decide how to **respond** and **recover** to the cyber incident. Managers and executives facilitate the work of the experts and allow them to concentrate on their expertise.

Currently there is a shortage of skilled cyber security professionals. For instance, in Europe it is estimated that there is a shortage of 291,000 cyber security professionals (ISC, 2019, p. 8). Most organizations are struggling to find skilled cyber security professionals. Hence, it is likely that during a major cyber incident, an organization has to hire external cyber security professionals, either from companies specialized in cyber security or independent contractors. External companies would then take the lead in responding and recovering to the cyber-attack (NCSC, n.d.). While these external contractors and consultants do have the required cyber

security skills, is its disadvantageous that they do not fully know the organization. Despite this decision-making power is deferred to these experts and they dictate how to **respond** and to **recover** from the cyber-attack.

Deference to expertise				
During a cyber-attack, (external) cyber security experts take the lead				
Identify	**Protect**	**Detect**	**Respond**	**Recover**
			x	x

2.3.6 Conclusion

In this section the meaning of the principles of HRO theory were further refined and specified (conceptualized). It was discussed if the functions of the NIST framework core could be applied to the principles of the HRO theory. In table 1 the findings of this section are summarized. It shows that the five functions of the NIST framework are 'covered' by at least one of the five principles of the HRO theory. This leads to the conclusion that, from a theoretical perspective, the principles of HRO theory can be used in research on cyber security. In the next chapter a case study is presented in which is analysed to what extent the principles of HRO theory are used in the cyber security of a hospital.

	Conceptualization	**Identify**	**Protect**	**Detect**	**Respond**	**Recover**
Preoccupation with failure	The preoccupation with failure to identify vulnerabilities and detect irregularities and anomalies	x		x		
Reluctance to simplify interpretations	High pace of innovation and creativity among cyber-attackers. Only way to keep up is the constant challenging of an organization's methods and assumptions.	x		x		
Sensitivity to operations	There has to be sharing of threat intelligence and all employees need a minimal level of cyber security awareness	x	x	x	x	

Commitment to resilience	Cyber resilience is the ability to respond to and recover from breaches in cyber security caused by cyber-attacks.				x	x
Deference to expertise	During a cyber-attack, (external) cyber security experts take the lead.				x	x

Table 1. Applying the functions of the NIST framework (horizontally) to the principles of HRO theory (vertically)

Chapter 3: Methodology

This chapter discusses the methodology of the research used for this thesis. In the first two sections it is discussed why a case study design has been chosen and also why a hospital has been selected as a case study. The third and fourth sections are a discussion on the main methods of data collection in this thesis. The last section discusses the operationalization of HRO theory so it can be used in the case study.

3.1 Why a case study design?

Yin (2009, p. 8) identifies several situations in which a case study design should be adopted; (1) when a 'how' or 'why' question is being asked, (2) when contemporary set of events is researched and (3) when the researcher has little or no control over the researched event.

The research question in this thesis is a 'to what extent' question. In the process of getting an adequate and full answer to this type of question one also need to ask 'how' and 'why' questions. So, in this case, if one finds clues that HRO principles are incorporated into cyber security, *how* and *why* questions are needed to fully analyse the extent of the incorporation. It is without doubt that cyber security is a contemporary phenomenon. As already emphasized in the previous chapters society increasingly relies on digital processes and systems; securing these processes and systems is key. Finally, for the case study in this study an independent organization is analysed. It is clear that the researcher has in no way control over this organization.

The case study design makes it possible to gain an in-depth understanding of how an organization cyber secures itself and especially if, and the extent to which, the principles of HRO theory have been incorporated in cyber security. While generalization is not possible due to the fact that only one organization was researched, insights on the possible added value of applying the HRO principles to cyber security can be gained. From this insight recommendations for future research can be formulated.

3.2 Case study selection

The selected case study is the cyber security in a Dutch hospital. The main criterion for the selection of this case study has been access (Yin, 2009, p. 26). In the hospital, the author has existing contacts who were helping in setting up the interviews for the case study. Since the main method of data collection is interviewing, the selected organization must allow their employees to be interviewed. Furthermore the selected organization must also be willing to

share their internal cyber security policy with the researcher. Many organizations were reluctant to allow this; the hospital was willing to do so.

A case study of a hospital is interesting, because HRO theory has already been implemented in health care. Examples of this are Bagnara, Paralengeli & Tartaglia (2010) and Dixon & Shofer (2006). Since the health care sector has experience with HRO theory, it is more likely that some principles from HRO theory has already been incorporated in their cyber security policy. This can provide an interesting perspective on the incorporation of HRO theory in cyber security. Furthermore, hospitals have been subject to cyber-attacks, such as an attack on Australian hospitals (Austrlian Associated Press, 2019) and the British National Health Service (Graham, 2017). The cyber threat for hospitals is real. Therefore, they should take cyber security seriously.

3.3 Data collection

Two data collection methods are used in this thesis: document analysis and interviews. First, documents are used to describe the circumstances in which the case study organization operates in. For example legal circumstances, such as the General Data Protection Regulation (GDPR). Also, documents can provide insights on how organizations already have incorporated HRO theory in its cyber security policy. As mentioned these documents contain sensitive information and gaining full access to these documents can be problematic (Yin, 2009, pp. 101-105). Therefore, a second method of data collection is needed; interviewing. A total of three individuals from the hospital were interviewed. In this thesis the in-depth interview type was used. In this type of interview, the interviewer can ask both about facts and opinions. This allows to go ‘deep’ into the subject matter (Yin, 2009, p. 107).

3.3.1. Document analysis

Document analysis is an often-used method in case study research. The main strengths of using document analysis for case studies are: (1) documents do not change and can be viewed repeatedly, (2) documents are unobtrusive, (3) documents are exact and (4) documents have a broad coverage. All of these factors allow analysis of a broad set of factors from different perspectives. It helps in triangulation and can counterbalance possible bias introduced by other research methods (such as interviewing). While there are some clear strengths of documents analysis, there are weaknesses as well: (1) retrievability can be issue since documents might be difficult to find, (2) selection bias and reporting bias, and (3) access to specific documents can be problematic. Selection bias is caused by the fact that the available and selected documents

are usually aligned with organization's policies and with the organization's principals. They may also reflect the emphasis of the particular organizational department that handles document-keeping. Reporting bias is present when a document reflects the (unknown) bias of the author of a document. Information about cyber security policy is often sensitive which often limit access to this information (Yin, 2009, p. 102).

In the research presented in this thesis, documents were used for two purposes. First, documents helped in describing the context in which the case study organization operates. Second, documents were used for the analysis of the extent to which principles of HRO theory were implemented in the formal cyber security policy of the case study organization.

3.3.2. Interviews

Interviews have strengths and weaknesses. The main strengths are: (1) interviews allow to directly target the case study topics and (2) interviews can be insightful, because interviewees can be asked for explanations. Interviews specifically help in answering the 'why' question (Yin, 2009, p. 102). Despite the strengths of interviews, there are certain weaknesses that require acknowledgement. First, bias is an issue in an interview and limiting this bias is a priority. Both the interviewer and the questions can be biased, as well as the interviewee. Interviewer bias can be limited by letting the interview questions be checked by others and by asking only open questions during the interview. Interviewee bias can be countered by asking for further explanation (by using short 'why and how' follow up questions), but interviewee bias always remains an issue. A second weakness is the occurrence of inaccuracy due to poor recall by the interviewer. For this thesis, all interviews will be recorded with approval of the interviewee. If the interviewee does not approve of recording, the interviewer will make extensive notes. The third and last weakness is reflexivity. Reflexivity means that the interviewee gives what the interviewer wants to hear. By making use of short 'why and how' follow-up question, reflexivity can be limited (Yin, 2009, p. 102).

The interviews are the key method of data collection for this thesis. The interviews are semi-structured; using this method facilitates discovery in a structured form. This allows the interviews to follow the structure of the five principles of HRO theory (Gillham, 2005, p. 72). The subjects covered during the interviews must be similar. By using prompts, equal coverage of the important subjects during the interviews is assured. When interviewees do not address certain aspects of a question, a simple 'what about' question is asked to assure coverage of all

relevant subjects (Gillham, 2005, p. 70). This allows for better comparison of the interview results. The interview questions are an annex to this thesis.

The interviews are in Dutch. The reasons for this is that both the interviewer and the interviewee are Dutch. Speaking in the mother tongue is more comfortable for both. The interviewees all work in the hospital in the IT department. Their functions are: manager computerization & automation, IT manager and Chief Information Security Officer (CISO). All interviews have been recorded and the transcripts are an annex to this thesis. Since some of the information is sensitive, the interviews have been anonymized. Hence, the identity of the interviewees and the hospital they work has been redacted. Furthermore, references to the suppliers of specific tools and software have also been redacted to more generic terms such as 'an antivirus' and 'a Security Operations Center (SOC)'. Lastly, these interviews have been slightly edited for clarity and readability purposes.

3.4 Data analysis

The main method of data collection for the research in this thesis are the interviews. Interviews result in large quantities of information which needs to be properly analysed. Coding is one of the methods that is very useful in analysing large quantities of textual data and helps to structure data for this analysis. For coding a codebook is required which provides structure to the coding. Since the interviews focus on the role of HRO theory in cyber security, the codebook is in line with the conceptualization of HRO theory (Gillham, 2005, pp. 137-140) as discussed in chapter 2. The codebook consists of five categories which are the same as five the organizing principles of HRO theory: preoccupation with failure, reluctance to simplify interpretations, sensitivity to operations, commitment to resilience and deference to expertise. Each of these categories include a definition (the conceptualization) and several indicators (operationalization). No separate codebook has been created since the codebook contains the same information as presented in table 2 at the end of this chapter. Each code has its own color. This color coding is used for coding the interviews. See the annex for the interviews including the color coding and a legend on the color of each category. This color coding allows for a structured analysis of the interviews.

3.5 Operationalization

Operationalization is the process by which a researcher specify how a concept can be measured. It's main purpose is to remove vagueness and making sure that concepts are measurable. So,

the process of operationalization is needed to make the conceptualized versions of the HROs organizing principles measurable. This section describes and discusses the process of operationalization for each of five organizing principles of HRO theory separately.

3.5.1 Preoccupation with failure

In the previous chapter, 'preoccupation with failure' was further specified as 'the preoccupation with failure to identify vulnerabilities and detect irregularities and anomalies". It was concluded that there is a need to identify vulnerabilities and a need to detect irregularities and anomalies that can be indications of unauthorized third party access to the system. Continuous searching for vulnerabilities and anomalies is crucial in any organization. This can be accomplished from inside, as well from outside, the organization.

Errors and warnings often are indications of vulnerabilities and these always need to be taken seriously. In this, a 'internal' culture in which it is encouraged to look for vulnerabilities and to report errors, is important. Such a culture can be created by rewarding the reporting of errors. Even if an individual reports an error caused by his/her own actions, the reporting should be rewarded, not punished. In an open and safe culture employees are able to speak freely on problems they see and errors they have made. Furthermore, close-calls are not seen as situations in which eventually things went well, but as situations in which it almost went wrong. These close-calls are an opportunity to identify vulnerabilities and detect irregularities, which improves cyber security (Weick & Sutcliffe, 2007, pp. 101-103).

External identification of vulnerabilities is also an option. 'White-hat' (or ethical) hackers can be asked to try to find any vulnerabilities in the cyber security system of the organization. This reporting of vulnerabilities by external parties is (financially) rewarded and known as responsible disclosure. Today, many organizations have a Coordinated Responsible Disclosure (CVD) program in which they (financially) reward the responsible disclosure of vulnerabilities by external parties (NCSC, 2018). Specialized companies can now be hired to perform a 'penetration' test to test an organization's cyber security. Penetration tests vary in size and complexness and beforehand arrangements must be made about the scope of the penetration test. After a test has finished, the penetration tester reports any vulnerabilities that have been identified (NCSC, 2017). The frequency of penetration tests varies; the advice is to do penetration testing at least annually and each time significant changes have been made to a system (Samarati, 2017).

Besides the identification of vulnerabilities, it is also necessary to detect irregularities and anomalies. Constant monitoring of the network allows for swift detection of any inconsistencies. Most organizations either create a Security Operations Center (SOC) or hire an external supplier of SOC services. There are varying degrees of monitoring. However, in essence a SOC monitors who accesses the network and monitors and all traffic on that network. Any irregularities or anomalies are closely analysed for indications of unauthorized third party access (NCSC, 2017). The creation or contracting of a SOC can greatly benefit the detection of unauthorized activity on the network.

	Conceptualization	**Operationalization**
Preoccupation with failure	The preoccupation with failure to identify vulnerabilities and detect irregularities and anomalies.	- Reward for the reporting of errors, vulnerabilities and anomalies, no punishments - Open discussion of problems - Close-calls are carefully analysed to find vulnerabilities - A CVD program exists - Yearly penetration testing or after significant changes to a system - The detection of irregularities and anomalies through a SOC

3.5.2 Reluctance to simplify interpretations

In chapter 2 the 'reluctance to simplify interpretations' was conceptualized into making critical analysis to identify and detect new cyber-attack methods and techniques. Since the adversaries are highly innovative and creative, cyber security needs also to be innovative and creative. Only by being critical and a constant challenging of the status quo, is it possible to keep up with ingenuity of the adversaries. To do this it is important to create an organizational culture in which nothing is taken for granted. Skepticism and constant questioning of assumptions and common practices are encouraged. It helps if a multidisciplinary cyber security team can be

created consisting of cyber security professionals with different expertise and people who have a good understanding of an organization's core business. People with different backgrounds and expertise approach problems differently which results in a better understanding of the problems. Asking questions and expressing unorthodox opinions is encouraged. Every opinion is taken seriously. This can provide unexpected insights into a problem. Furthermore, every incident is carefully analysed to better understand the methods of threat actors and to learn how to protect against these (Weick & Sutcliffe, 2007, pp. 103-105). Creating this culture can improve the identification and detection capabilities of organizations. This can greatly benefit an organization's cyber security.

	Conceptualization	**Operationalization**
Reluctance to simplify Interpretations	High pace of innovation and creativity among cyber-attackers. Only way to keep up is the constant challenging of an organization's methods and assumptions.	- Constant questioning of assumptions is encouraged - Diverse team, consisting both out of cyber security experts and 'normal' employees - Extensive analysis of every cyber incident

3.5.3 Sensitivity to operations

In the previous chapter, 'sensitivity to operations' has been conceptualized into: (1) organizations need to be aware of the risks and current cyber security issues by having good threat intelligence and (2) in the whole organization a minimal level of cyber security awareness must be present. This allows an organization to better identify the risks, protect itself against these risks, detect intrusions and respond to these.

First, an organization must have a clear picture of the main cyber threats. This allows the organization to better prepare themselves for known threats and identify new threats. In order to do this the so called threat intelligence must be shared. Second, all employees are expected to have a minimal level of cyber security awareness. Ideally, every employee undergoes regular cyber awareness training in which they are informed about the common and simple cyber-attacks that they are likely to encounter. Also, a set of rules about basic security practices must be widely introduced in the organization. Examples are password management and not leaving

USB thumb drives unattended. These basic rules have to be understandable for all employees and can greatly improve cyber security. Improving the security awareness is a continuous process that never stops. Regular reminders and testing of the employees is necessary to keep the level of awareness at a stable level (Wilson & Hash, 2003). Cyber security should always be a key factor in the daily work of all employees (Weick & Sutcliffe, 2007, pp. 105-106). Knowing, understanding and being aware of the risks in cyber space allows for better identification of vulnerabilities, benefits protection against cyber-attacks, improves the ability to detect unauthorized access and betters the ability to respond to cyber-attacks.

	Conceptualization	**Operationalization**
Sensitivity to operations	There has to be sharing of threat intelligence and all employees need a minimal level of cyber security awareness	- Clear picture of the main threats - Sharing threat intelligence - Cyber security awareness training for all employees - Basic cyber security rules for all employees - Testing of employees' cyber security awareness - Reporting of possible cyber-attacks - Cyber security professionals should be around for consultation and recommendations

3.5.4. Commitment to resilience

The 'commitment to resilience' conceptualizes into cyber resilience, which is the ability to respond to and recover from cyber-attacks. Multiple objectives have been identified for cyber resilience: continuation of operations, constraining the impact, reconstitution of systems and processes, and an evaluation that results in improvements of an organization's cyber security. Committing to resilience greatly helps in the preparation for responding to and recovering from cyber-attacks.

An adequate response to a cyber-attack requires a skilled group of people. Since the impact of the attack is often unknown, these people must have the ability to learn quickly and constantly test what methods are successful in countering a cyber-attack. Regular training and testing is required to develop these skills and to keep these at a high level. Also, the cyber security experts must have a broad understanding of cyber security. This allows them to help their colleagues whenever necessary (Weick & Sutcliffe, 2007, pp. 107-108). Weick & Sutcliffe (2007, pp. 67-73) warn for the negative effects of anticipation. A high degree of anticipation could result in disregard of the unanticipated. Having a contingency plan on how to respond to and recover from cyber incidents is recommended. However, in this plan there should be sufficient space for improvisation and creativity. When necessary, diverting from the plan is accepted.

During an cyber-attack, it is essential that reserve resources are available that can be used to (temporarily) replace damaged systems and allow operations to continue. Furthermore, immediate backups of all non-damaged systems need to be made. In this way, information can be saved and later used to reconstitute damaged systems. These back-ups must be made at least daily and more frequent back-ups are obviously better (Ross, Pillitteri, Graubart, Bodeau, & McQuaid, 2019, p. 90).

After a cyber-attack has been constrained, and all systems and process have been reconstituted, an extensive evaluation must be carried out. Lessons learned can be implemented to improve cyber security.

	Conceptualization	**Operationalization**
Commitment to resilience	Cyber resilience is the ability to respond to and recover from breaches in cyber security caused by cyber-attacks.	- Reserve resources that can be allocated in times of need - Daily backups of all systems - The crown jewels have been identified - Broad understanding of cyber security among cyber security professionals. - Real-time learning and creativity are valued

		- Training and testing of cyber resilience - After an cyber incident, assessment of the incident - Lessons learned must be implemented - A contingency plan that allows for creativity and improvisation

3.5.5. Deference to expertise

During a cyber-attack, the HRO theory states that there should be deference to expertise in times of high stress on an organization. This principle was conceptualized in chapter 2 to a deference of cyber security expertise during a cyber-attack. Operationalizing the 'deference to expertise' to the cyberspace, means that decision-making power is delegated to the person who is most qualified. During a cyber-attack this is probably a cyber security expert. The most qualified person has the authority to make impactful decisions. In these cases, expertise is valued more than hierarchy. If this expertise is not present in an organization, external expertise can be brought in (Weick & Sutcliffe, 2007, pp. 109-110). Nowadays the expertise is more likely to come from external parties due to a shortage of cyber security personnel. These external contractors are more likely to have specific skills that is lacking in an organization. Cyber security experts possess the necessary cyber expertise to decide on the response to and recovery from a cyber-attack. Thus, they should have the decision-making power to do so.

	Conceptualization	**Operationalization**
Deference to expertise	During a cyber-attack, (external) cyber security experts take the lead.	- During cyber-attacks, most qualified person gains decision-making power - If expertise is missing, external expertise is brought in

Conclusion

This methodology chapter has set out why a case study design is appropriate for this research and why the case of a hospital has been selected. The pros and cons of the two methods used for data collection (document analysis, interviewing) are discussed. Lastly, each of the organizing principles of HRO theory have been operationalized; an overview is presented in table 2.

	Conceptualization	**Operationalization**
Preoccupation with failure	The preoccupation with failure to identify vulnerabilities and detect irregularities and anomalies.	- Reward for the reporting of errors, vulnerabilities and anomalies, no punishments - Open discussion of problems - Close-calls are carefully analysed to find vulnerabilities - A CVD program exists - Yearly penetration testing or after significant changes to a system - The detection of irregularities and anomalies through a SOC
Reluctance to simplify Interpretations	High pace of innovation and creativity among cyber-attackers. Only way to keep up is the constant challenging of an organization's methods and assumptions.	- Constant questioning of assumptions is encouraged - Diverse team, consisting both out of cyber security experts and 'normal' employees - Extensive analysis of every cyber incident
Sensitivity to operations	There has to be sharing of threat intelligence and all employees need a minimal	- Clear picture of the main threats - Sharing threat intelligence

	level of cyber security awareness	- Cyber security awareness training for all employees - Basic cyber security rules for all employees - Testing of employees' cyber security awareness - Reporting of possible cyber-attacks - Cyber security professionals should be around for consultation and recommendations
Commitment to Resilience	Cyber resilience is the ability to respond to and recover from breaches in cyber security caused by cyber-attacks.	- Reserve resources that can be allocated in times of need - Daily backups of all systems - The crown jewels have been identified - Broad understanding of cyber security among cyber security professionals. - Real-time learning and creativity are valued - Training and testing of cyber resilience - After an cyber incident, assessment of the incident - Lessons learned must be implemented - A contingency plan that allows for creativity and improvisation

Deference to expertise	During a cyber-attack, (external) cyber security experts take the lead.	- During cyber-attacks, most qualified person gains decision-making power - If expertise is missing, external expertise is brought in

Table 2. Overview of the conceptualization and operationalization of the five principles of the HRO theory.

Chapter 4: A case study on the extent of incorporation of the principles of HRO theory in a hospital's cyber security

In chapter 2 it was argued that, from a theoretical perspective, the principles from HRO theory can be 'translated' to cyber security. However, to 'test' this it is necessary to go to the practice. This chapter describes a case study of a hospital's cyber security. The analysis of the cyber security policy of this hospital is primarily based on interviews with three IT employees from the hospital who are all involved in making the hospital cyber secure. In this chapter referrals are made to the transcripts of the interviews with these employees; 'Interview 2, 303-305' refers to line 303-305 of the transcript of the interview with employee number 2. When necessary, documents and online sources are used for additional information or clarification. The structure of this section follows the five organizing principles of the HRO theory. After a short discussion on why cyber security is important for hospitals, the incorporation of each of the five organizing principles of HRO theory in the hospital's approach to cyber security is analysed.

4.1. Why does a hospital has to be cyber secure?

In hospitals, cyber security is required for two reasons: the continuation of operations and for safeguarding privacy. First, hospitals must be able to operate 24 hours a day, 7 days a week and 52 weeks a year. In the case of medical emergencies, any hindrance in digital systems can be literally deadly. For patient care, hospitals increasingly rely on systems that include, or are based on, information technology. These systems can be roughly divided into two groups: medical devices and management systems. Medical devices are used to treat patient and to gather diagnostic information (e.g. EKG-monitoring). Management systems are used to collect and share information (e.g. Electronic Health Record). Since many of these systems use information technology that is connected to the outside world, there is a significant cyber security risk. Hacking of these systems endangers the continuation of operations in a hospital. When medical devices are hacked, the device provides inaccurate diagnostic information or doesn't perform accurately (e.g. syringe pump). Also, it is possible that a hacked medical device does no longer function at all (De IT-Auditor, 2015). Management systems must provide accurate information whenever necessary. Without the availability of accurate information, providing safe and efficient medical care becomes problematic. When a management system has been accessed by a hacker, there is serious risk that information is not available or inaccurate. For the continuation of operations in a hospital, it is crucial that medical devices and management systems are adequately protected against cyber-attacks.

Second, cyber security in a hospital is required for safeguarding privacy. Hospitals possess large quantities of medical (and thus sensitive) data. Nowadays all of these data are saved digitally. Hence, good cyber security is required to prevent unauthorized access to these sensitive data. Besides medical data, hospitals possess large quantities of personal information on patients, such as names, addresses, email addresses, BSN-numbers, information on insurance etc. Leaking of this personal information can have significant consequences for patients. Since the introduction of the GDPR, the emphasis on privacy has increased. Organizations that store personal information are required to take adequate steps to secure these data. When an organization fails to do so, hefty fines can be handed out by the responsible authorities (Zerlang, 2017).

4.2. Preoccupation with failure

The first organizing principle of the HRO theory is the preoccupation with failure. In chapter 2 this was conceptualized as the preoccupation with vulnerabilities and anomalies. Being preoccupied with failure, allows for the early identification of vulnerabilities and detection of anomalies. This identification and detection can be done by the hospital itself or by external partners. In the following sections itsis explained how the hospital identifies vulnerabilities and detects anomalies, both internally and externally. First, the role of the hospital's own employees is analysed. Second is an analysis of vulnerabilities and how external parties help in identifying these. It is also discussed why the number of existing vulnerabilities is relatively high in the hospital's network. Third, is a discussion on the detection of anomalies and the role of external parties in this process.

4.2.1. The preoccupation of failure among hospital employees

Internally in the hospital, finding vulnerabilities is predominantly done by the IT team. While other employees, such as doctors and nurses, do report IT-related problems, these reports usually concern malfunctioning of IT systems, not security issues. Nonetheless, reporting of malfunctioning systems is essential for cyber security, because malfunctioning can be an indication of a security breach or vulnerability (Interview 2, 303-305). Employees can report IT issues by calling the IT-helpdesk. If a problem is possibly linked to a security issue, the CISO (Chief Information Security Officer) is contacted for further analysis and action if necessary (Interview 3, 559-660). Furthermore, employees can file VIM reports. VIM stands for 'Veiligheid & Incident Meldingen', which translates to 'Security and Incident Reports'. This is a general reporting system for all kinds of incidents. This ranges from reporting

inappropriate behavior to medical (near) misses. This system can, in theory, also be used for reporting (cyber) security issues (Interview 1, 133-136).

Despite these structures, employees barely report any specific cyber security issues. When they do report, it is usually only about a suspicious e-mail (Interview 3, 550-551). Several explanations can be thought of for this low level of reporting. First, the reporting of specific cyber security issues by employees is not rewarded (nor punished). So, there is no incentive (positive or negative) to report any issues. Second, the reason that people work in the healthcare sector Is that they want to help and care for people. Their focus is on doing this well and they in general don't have a high level of awareness when it comes to cyber security (Interview 3, 615-618). Cyber security requires a more skeptical and suspicious mindset than is present under the hospital employees. It would help if an open discussion about cyber security issues is actively promoted. Third, employees simply do not have sufficient expertise to recognize potential cyber-related vulnerabilities and anomalies. They lack knowledge about cyber security. The high success rate of phishing (Interview 2, 326-328) in the hospital supports this claim.

Partly due the failure of employees to identify vulnerabilities and to detect anomalies, there have been several instances in which a large security breach almost happened. An example of such a near-miss was when the external connection between the hospital systems and the radiologist home computers was found to be insecure (due to a failure in a decryption tool). This external connection is used by the on call radiologist to analyse scans of patients from home which allows for quicker (and possible life-saving) diagnosis. At first this vulnerability was considered to be non-urgent. However, the urgency quickly changed when the hospital-CERT received new threat information. It was decided to immediately disable the external connection and the vulnerability was patched (Interview 2, 423-439). Since the initial response to this vulnerability was slow, external parties informed the hospital-CERT that it was likely that the vulnerability already was exploited. After an investigation, luckily it was found that this had not happened (Interview 3, 556-560). Afterwards, it became clear that the warning about the insecure connection was received on time, but was not prioritized properly. Every week the hospital receives about 50 to 80 warnings and threat reports. The warning about the insecure external connection was one among many. The prioritization of this warning was too late and too little. Only after this vulnerability was also detected in other organizations, the urgency increased (Interview 3, 563-570). Remarkably, the occurrence of this 'near miss' did not lead to implementing specific measure based on the 'lessons learned' from this incident.

4.2.2. Identifying vulnerabilities

All interviewees (Interview 1, 138; Interview 2, 377; Interview 3, 645) acknowledge that vulnerabilities exist in the hospital systems and network. It is without doubt that such a vulnerability can be exploited and cause a security breach. In order to limit the risk of exploitation of these vulnerabilities, the hospital actively tries to identify these vulnerabilities. Nonetheless, it is unlikely that all vulnerabilities will be found since the network is too complex to identify all the vulnerabilities. Also, due to the high pace of development of information and medical technology, new vulnerabilities arise constantly. Furthermore, complexity is added by the high number of (medical) devices and applications connected to the hospital's network. Many of these devices and applications are supplied by external parties. While the hospital is able to adequately secure its core systems, the many applications and devices that are connected to the network form a great security risk (Interview 1, 62-70). Cyber security is usually not the main priority during the design of many medical devices and applications. When connected to the hospital's network, this leaves the hospital vulnerable (Forescout, 2019, p. 8). In order to limit this risk, one member of the IT staff has been trained as a Certified Ethical Hacker. This employee tries to hack new medical devices and applications to identify vulnerabilities (Interview 2, 246-249). Despite these measures the number of vulnerabilities in the hospital is relatively high and patching these vulnerabilities is problematic. A number of factors play a pivotal role in this:

1. Many medical devices and applications run on legacy Windows Operating systems. For instance, Windows XP still is the operating system for many medical devices. Microsoft, the developer of all Windows operating systems, stopped supporting Windows XP in 2014. This means that security updates are no longer provided for Windows XP and new vulnerabilities remain unaddressed. The continued use of Windows XP is a high risk from a security perspective (Interview 1, 62-70).

   Other medical devices run on Windows 7. On the 14th of January 2020, Microsoft ended support for Windows 7. Updates will no longer be provided to patch vulnerabilities in this operating system. It is expected that the number of vulnerabilities will continue to rise (Interview 1, 66-67). A reason for the continued use of legacy operating systems, is that many vendors continue to choose to use specific (outdated) software, because they understand the strengths and weaknesses of that particular operating system (GAO, 2012, pp. 21-22).

2. When medical devices are first bought, they are certified for medical use. However, this certificate is only valid if the device stays in its current state. It is not allowed to modify the device, also when this is needed for cyber security reasons. So, when new vulnerabilities are found, these cannot be patched, because patching results in a device which is no longer in its original state. This mean that the device is no longer certified and can no longer be used for the treatment of patients (Interview 3, 700-703). Furthermore, many suppliers do not allow to run virus scanners on their medical devices. The suppliers argue that a virus scanner can hamper the performance of the medical device. This leaves a device vulnerable to external cyber-attacks (Interview 1, 62-70).
3. The network of a hospital is immense. Many devices and application are connected to the hospital's network. Examples of devices connected to the network are, syringe pumps, X-ray scanners, emergency generators, Electronic Health Record Systems, printers and many others. Each one of these devices are a pathway for malicious actors to access the hospital's network. The network is simply too big to be completely secure (Forescout, 2019, p. 3). The challenge that comes with the size of the network is exemplified by long list of hundreds of vulnerabilities that the hospital receives after a penetration test. Obviously, the most urgent issues are first addressed and resolved. However, that leaves many more issues initially unattended while in the meantime new problems arise; 'It is a never ending story' (Interview 2, 255-260).
4. Software updates of the medical devices itself, addresses vulnerabilities and other security issues. When these are not (timely) carried out, the security risk increases. However, updating the software of the device is not so straight forward as it commonly is considered. Most of the devices and applications are configured for a specific software version. This configuration is needed for proper functioning of all the interconnected devices and applications. When a software update for a device is installed, it is possible that this device can no longer be configured with the required specific settings. This would mean that the device or application can no longer be used, which would greatly hamper the hospital's operations. Alternatively, one can choose not to perform the software update but this leaves the network more vulnerable to cyber-attacks (Interview 2, 286-293).

A hospital network is too large and too complex to only rely on internal identification of vulnerabilities. Therefore, external partners are hired to help. The hospital goes through regular

penetration testing (at least once a year). The goal of a penetration test is to find weaknesses in an IT system (NCSC, 2017). For two to three weeks the external testers try to gain access to the hospital's network (Interview 2, 250-253), both digitally and physically. Digitally, the testers attempt to find as many vulnerabilities without physically accessing the hospital, for example by scanning the network for these vulnerabilities. Physically, the testers try to gain access to restricted areas of the building. When they have gained access, they can, for example, use an unattended personal computer to access the network or install malicious software. To gain access, testers often take on different identities. One tester, posing as a new medical student, managed to be invited to watch a surgical procedure. This should of course not be possible at all (Interview 1, 111-115). After a penetration test the testers write a report about the problems and vulnerabilities they encountered. Each vulnerability is labeled with a level of urgency. It is then up to the hospital to address these vulnerabilities (Interview 2, 253-260).

Penetration tests are becoming standard practice for many organizations. These tests are now often also required by regulation or for certain certifications. For instance, the hospital is required to do regular penetration testing as part of the Digi-D audit. Digi-D is an identity management platform used by Dutch government agencies to digitally verify the identity of Dutch residents; it functions as a digital ID. The hospital uses Digi-D for patients to log in to the patient portal. When using Digi-D, strict security measures need to be taken and every year the requirements become more stringent. The downside of this is that it is for the hospital quite labor-intensive to implement all the these new security requirements. But, on the upside, by implementing these requirements the level of the hospital's cyber security is increased altogether (Interview 1, 82-86).

Many organizations have implemented Coordinated Vulnerability Detection (CVD) Programs. Remarkably, one of the interviewees states that the hospital has a CVD program (Interview 2, 269-271) but this could not be confirmed by one of the other interviewee (Interview 1, 44). However, a CVD program does indeed exist and can be found on the hospital's public website (a link to the website cannot be provided, because it would reveal the hospital's identity). So far, only two reports have been filed. The actors who filed these reports differ. It can be from companies looking for a contract, but also from script kiddies, who use specific programs to find vulnerabilities (Interview 2, 269-275).

4.2.3 Detecting anomalies

While identifying vulnerabilities helps in protecting against known cyber-threats, not all vulnerabilities can be identified or addressed. Therefore, the likelihood of malicious third parties accessing the hospital's network remains high. In order to limit the damage that these malicious actors can do, it is necessary to detect their presence early. Early detection enables an early response and containment of the cyber-attack. As a result of the presence of action of a unauthorized third party, systems and medical equipment can malfunction. If this happens the hospital employees working with these systems and equipment, report the malfunctioning to the IT helpdesk (Interview 3, 553-554). However, most malfunctioning caused by intrusions are not detected by the hospital employees, but by a specialized external partner. The hospital has outsourced the detection of anomalies to an external Security Operations Center (SOC). The SOC has placed multiple sensors on strategic places in the network. Through these sensors the SOC monitors the hospital's network 24/7 for any anomalies. Whenever they detect unusual data traffic, they analyse this anomaly. If the SOC concludes that an anomaly is likely caused by presence and actions of an unauthorized third party, they contact the hospital-CERT. The hospital-CERT continues the analysis and decides on further actions (Interview 2 Hospital, 391-402).

4.2.4 Conclusion

Internally, the preoccupation with failure in the hospital is low. Employees do rarely report any errors and failure and there is no reward for reporting. The cyber security team has insufficient resources relative to the size and complexity of the hospital and relies heavily on external partners for the identification of vulnerabilities and detection of anomalies. The hospital has partnered with a penetration testing company and a SOC. One can state that the hospital for most part has outsourced its connection with the principle of preoccupation with failure. To what extent the principle of preoccupation with failure has been incorporated in the hospital external partners could nog be established.

Referring to table 2 the extent of the incorporation of the principle of preoccupation of failure can be summarized as follows:

Operationalization	**Incorporated?**	**Remarks**
Reward for the reporting of errors, vulnerabilities and anomalies, no punishments	No	

Open discussion of problems	Not obvious	
Close-calls are carefully analysed to find vulnerabilities	Yes	Only the most urgent close-calls are analysed (and patched if necessary)
A CVD program exists	Yes, but not well known	Even in the IT department itself not everyone knew that it existed
Yearly penetration testing or after significant changes to a system	Yes	
The detection of irregularities and anomalies through a SOC	Yes	

4.3 Reluctance to simplify interpretations

The pace of innovation in cybercrime is high. Cyber-attackers constantly come up with new methods to gain unauthorized access to a network. The task of cyber security professionals is to prevent this from happening. In order to keep up with cyber criminals, being reluctant to simplify interpretations is required. Cyber security professionals always should have a skeptical attitude to the status quo. According to HRO theory, having a divers cyber security team consisting both out of cyber security experts and 'normal' employees, helps in creating this skepticism. People with different backgrounds analyse a problem differently. Therefore, the analysis of a problem can be more extensive and can result in helpfull insights. A skeptic attitude is necessary to better understand incidents and failure, and helps in the early identification and detection of vulnerabilities and anomalies.

4.3.1. The internal reluctance to simplify interpretations

The hospital-CERT is the organization in the hospital responsible for cyber security. The CERT consists of four people: the CISO (Chief Information Security Officer), manager IT and two individuals from the IT staff ((Interview 2, 308-309). All members of the CERT have an IT background; it is a small and homogenous group. There is little diversity in expertise and background (Interview 3, 583). Thus, it can be argued that the CERT's understanding of a problem is limited, because they primarily analyse it from an IT perspective. According to HRO theory, the inclusion of non-IT employees would likely result in a better understanding of a problem.

Furthermore, not every problem or incident is fully analysed. Every week the hospital-CERT receives about 50 to 80 threat reports. The hospital-CERT has insufficient resources to fully analyse each one of these threat reports. Only the most urgent threats are analysed and acted upon (Interview 3, 567-575). The workload for the cyber security experts is simply too high. Besides handling the aforementioned threat reports they also have to implement new security policies, apply for certain certificates (e.g. NEN7510 and DigiD) (Interview 1, 92-95), perform penetration testing of new medical equipment and systems (Interview 2, 246-249) and many other tasks. In short, the hospital-CERT is too small, relative to the workload, to fully analyse every incident or problem. They cannot internally fulfill the requirement of being reluctance to simplify interpretations.

4.3.2. The external reluctance to simplify interpretations

Since the hospital itself has insufficient resources, it seems that most of the required skepticism when handling cyber security problems has been outsourced. A first example of this is the fact that the hospital relies on external suppliers which provide security services and products (e.g. a firewall and antivirus software). These suppliers release regular updates of their products (Interview 2 Hospital, 494-497). The suppliers must keep up with the newest developments in cybercrime and cyber-attack methods which requires a constant skepticism to the status quo. A second example is the external SOC. The SOC constantly monitors the network for any anomalies. When an anomaly is detected, it is extensively analysed. When the SOC considers the anomaly to be serious, the Hospital-CERT is contacted for them to act (Interview 2, 391-402). A SOC must be reluctant to simplify interpretations; they carefully analyse every change in data traffic to determine its cause. A third example is the yearly penetration test. During such a test, the testers try to find weaknesses in the hospital's cyber security. Since new weaknesses arise constantly, penetration testers must keep up with this (Interview 2, 250-253) for which requires a certain amount of skepticism is needed. Only by being reluctant to simply interpretations the testers can identify weaknesses in their clients' cyber security.

4.3.3 Conclusion

The reluctance to simplify interpretations is missing in the hospital-CERT. First, this team is homogenous and, second, it is insufficiently staffed to analyse every incident. It seems that the hospital has outsourced most of the needed reluctance to simplify interpretations to external partners.

Referring to table 2 the extent of the incorporation of the principle of reluctance to simplify interpretations can be summarized as follows:

Operationalization	**Incorporated?**	**Remarks**
Constant questioning of assumptions is encouraged	Not obvious	
Diverse team, consisting both out of cyber security experts and 'normal' employees	No	The CERT consists only of IT-experts
Extensive analysis of every cyber incident	No	The workload of the CERT is too high

4.4 Sensitivity to operations

To ensure good cyber security, having awareness about cyber security issues is key. Gathering and sharing of threat intelligence helps in creating this awareness. However, this awareness must be present among all employees and not only in a cyber security team. So, everyone in the hospital must have a minimal understanding of the risks involved in cyber security. This allows them to recognize and adequately respond to cyber threats. In other words, the hospital and its employees must be sensitive to the operations of cyber security. In the following sections the hospital's sensitivity to operations is discussed. The first section analyses how threat intelligence is gathered form external sources. The second section describes the role of employees in the cyber security process. The third section is a discussion of the hospital's efforts to improve cyber security awareness among employees. Fourth is an analysis on other protective cyber security measures that the hospital has taken.

4.4.1. Sharing threat intelligence

In order to be aware about the most pressing and current threats, the hospital needs to have good intelligence gathering capabilities. Since the hospital has insufficient resources to do this independently, it is part of three 'threat intelligence sharing' networks. First, the hospital's CISO is member of a network consisting of all CISOs of Dutch hospitals. This network is part of the Nederlandse Vereniging van Ziekenhuizen (NVZ), which is the Dutch Association of Hospitals, (Interview 1, 15-18). The NVZ network facilitates the sharing of experience and expertise (e.g. policy documents are exchanged for review (Interview 3, 594-595)) and this

network operates as an Information Sharing and Analysis Centre (ISAC). The Dutch National Cyber Security Centre takes part in this network (Schippers, 2016, p. 2). Second is Zorg-CERT. This is an organization that was founded in 2018 to improve cyber security in the medical sector (NOS, 2018). Zorg-CERT helps the medical sector to improve their cyber security and provides support during security breaches. Since Zorg-CERT is only active in the medical sector, it has useful specific expertise on the security of medical hardware and software (Z-CERT, n.d.). Another important task of Zorg-CERT is providing information and identifying new or changing threats. The hospital regularly receives updates on new or urgent threats from Zorg-CERT (Interview 3, 530-531). Third, the hospital has partnered with multiple external cyber security partners, for instance companies that provide antivirus scanners and firewalls. These companies constantly monitor digital networks for new threats. They first identify these new threats, then update their product to detect this new threat and if necessary implement measures to protect against this threat. Monitoring and updating is an indirect form of intelligence sharing that benefits the hospital. The constant updating is part of the service provided by the supplier to the hospital (Interview 1, 100-101).

So, multiple networks provide the hospital with intelligence on the most problematic and pressing threats. However, the high number of intelligence reports and warnings these networks generate is problematic. Every week, the CISO receives about 50 to 80 notifications about possible threats (Interview 3, 566). Since the hospital uses many different systems and applications, the CISO first has to decide whether any of these notifications apply to one of the hospital's systems and applications. Valuable time is lost in this process. Furthermore, the urgency of the intelligence varies. Some problems are more pressing than others and, due to the volatility of the cyber space, the level of urgency can change over time (Interview 3, 563-565).

4.4.2. The role of humans in cyber security

All employees of an organization must be aware of the importance of their organization to be cyber secure. However, in the hospital this is not the case. All interviewees agree that people are by far the weakest link in the hospital's cyber security (Interview 1, 104; Interview 2, 326; Interview 3, 597-603). The level of awareness about cyber security among the employees of the hospital is worryingly low. Consequently, employees take actions that allow malicious hackers to gain access to the hospital's network. A prime example is phishing in which employees are tricked by fake emails into clicking on links or opening attachments that contain malicious software. Even though employees are aware that they should not respond to phishing emails, they often fail to do so (Interview 2, 326-328). Phishing attacks are often successful,

because employees do not give the proper attention to the content of the e-mail. When employees are asked why they have clicked on a malicious link, it is often because they are in some kind of hurry. One victim said that he was going on vacation the next day and wanted to get through all his emails before he left. Another example, is a man whose mother had just passed away. Since he was dealing with the administrative aspects of her passing, he received many emails from different companies and organizations. He thought that the phishing email was also from one of these organizations. Hence, he fell for the trickery of the phishers (Interview 2, 361-368).

Improving cyber security awareness in the health care sector is a challenge. A more skeptical and suspicious attitude is required. However, people that work in the medical sector are helping patients with an open and welcoming mindset, and are, in general, not very skeptical and suspicious by nature (Interview 3 Hospital, 614-617). As already mentioned it has happened that an external penetration tester, imposing as a medical student, was able to get himself invited by hospital employees to attend a surgical procedure! In this case the hospitability and friendliness of the employees resulted in a significant security risks (Interview 1, 111-115). One of the other main security threats is the problem that employees do not lock their personal computers when leaving their workplace. This means that an intruder can easily get access to sensitive patient information through unattended and unlocked computers (Interview 3, 601-603).

The employees of a hospital can also themselves violate privacy regulations (Interview 3, 123). All medical files are digitally saved in an Electronic Health Record System. Everyone with authorization can access these files. There is no barrier that prevents access to files of patients to which the employee has no medical responsibilities. While employees should not peek in files of patients they do not treat, this does happen. An example of such a violation of privacy happened in a hospital in The Hague. When a well-known reality TV-star was admitted in the hospital, a total of 85 employees looked in her file. Most of these employees did not have any good reason to do this besides satisfying their curiosity (AD, 2018).

4.4.3 Efforts to improve security awareness among employees

Since humans are the weakest link in the hospital's cyber security, the hospital is implementing programs to increase the awareness on cyber security. In this way the hospital tries to make the employees more resilient to cyber threats. One of these programs is aiming at improving awareness about privacy. It consists of posting of posters on the intranet with questions such as

‘The alderman is in the hospital, can I take a look in his files?’. The answer to this question is ‘no’ and of course all employees know this. However, it does remind employees about the regulations about privacy. There are plans to implement more extensive awareness programs, such as e-learning and serious gaming, but so far these have not been implemented (Interview 3, 609-613). Testing of the security awareness among employees does happen. Regularly the IT-department sends fake phishing emails to all employees. They should identify these emails as phishing emails but many fail to do so. During the last tests, about 30% of all employees clicked on the link in the phishing email and thus failed the test. When employees click on a phishing link or attachment, they immediately get a pop-up on their screen. This pop-up states that they have failed the test and provide information on how to recognize phishing emails (Interview 3, 625-627). Furthermore, they are urged to do an e-learning course on cyber security (Interview 1, 117-119). Despite these efforts, improving the awareness on cyber security in the hospital remains a challenge. Interviewee 3 expressed his doubts about the efficacy of these measures. Nonetheless, they must keep trying to improve awareness (Interview 3, 625-627).

Beside raising the awareness, the hospital tries to find technical measures to limit the damage from for example the phishing problem. Malicious software can easily be hidden in certain kinds of files such as ZIP files. These files use a form of encryption which makes that anti-virus software cannot recognize these files as being malicious. So, these phishing emails are not blocked by virus scanner and end up in the employees’ inbox. In order to limit the risk, emails containing certain attachments, such as ZIP files, are completely blocked. About 20 to 30 files types are now always blocked. This measure decrease the reliance on humans to detect phishing attempts.. However, it remains possible to circumvent these protective measures. Thus, the employees role remains important in the cyber security process. Since many employees fail to do so, a well-designed phishing attack in the hospital is likely to succeed (Interview 2, 338-347).

4.4.4 Additional protective measures

While the way in which employees act and behave is one of the most important vulnerabilities in the hospital’s cyber security in, other vulnerabilities are also important. These other vulnerabilities are difficult to address due to the use of old (and inflexible) systems and applications. However, not addressing these major vulnerabilities, leaves the hospital extremely vulnerable to external cyber-attacks. Thus, workarounds are needed that prevent the exploitation of the vulnerabilities. For this, the hospital uses the technique of what is called ‘virtual patching’ (Interview 2, 296-300). The Open Web Application Security Project

(OWASP) defines virtual patching as '*A security policy enforcement layer which prevents the exploitation of a known vulnerability'* (Barnett, Cornell, Hoffman, & Knobloch, n.d.). In contrast to actual patching, virtual patching does not change the source code of software, but it detects when attempts are being made to exploit a vulnerability. One of the advantages of virtual patching is that it does not interfere with the operations of a system. However, it does not fully address a vulnerability. Only the known methods of exploitation are addressed and any new or slightly different exploit might circumvent the virtual patching. While virtual patching is a good solution to address a vulnerability for some period of time, in the long run it is better to actually patch the vulnerability (Donaldson, 2014).

Another important protection measure is to have multiple layers of protection mechanisms in place. First, a firewall stands between the internal network of the hospital and the outside world. All traffic goes through this firewall. Second, every computer has it is own antivirus scanner. It is critical that the firewall and the antivirus are supplied by two different companies. The reason for this is that one supplier might only need a short time to identify a specific threat, another supplier might take significantly longer time to identify the same threat or not identify the threat at all. If only the second supplier's security software had been installed, the risk of a breach is higher (Interview 2, 491-497). Other layers are formed by the use of passwords, use of a Virtual Private Network and the use of encryption. It is necessary to use multiple techniques, because each one of these techniques can fail. Nonetheless, this does not make the hospital 100% cyber secure. The risk of a large security breach remains high. Interviewee 2 compares cyber security with a medieval castle. A castle consists of multiple security measures: a portcullis, a drawbridge, high walls and knights. Together these measures make a caste more secure. As in cyber security, a diverse set of security measures must be implemented (Interview 2, 497-501). However, too much security can hamper the operations of the hospital. For example, Choi et al. (2019) found that increased security measures increased the time needed to diagnose cardiac arrests. The reason for this was that all the security measures made that it took longer for hospital employees to log-in in the network and access critical information for the treatment of patients.

4.4.5 Conclusion

In general the sensitivity to the operations of cyber security among non-IT employees in the hospital is low. The Hospital-CERT is actively trying to keep up with the newest intelligence and the hospital is a member of multiple networks through which it gains intelligence on new and urgent threats. However, the cyber security team has insufficient resources to fully and

timely analyse all intelligence. Thus, it is possible that crucial intelligence is missed or misinterpreted.

Unfortunately the cyber security awareness among the employees of the hospital is minimal; the sensitive to the operations of cyber security is low. The hospital has taken small steps and measures to improve awareness. However, the efficacy of these measures is questionable and the low level of cyber security awareness remains an issue. The hospital tries to overcome this by installing protective measures such as the use of firewalls, antivirus scanners, passwords, Virtual Private Network and encryption.

Referring to table 2 the extent of the incorporation of the principle of sensitivity to operations can be summarized as follows:

Operationalization	**Incorporated?**	**Remarks**
Clear picture of the main threats	Yes and no	Intelligence gathering from multiple sources, but insufficient resources for good analysis
Sharing threat intelligence	Yes	
Cyber security awareness training for all employees	Minimal	
Basic cyber security rules for all employees	Yes	Adherence to these rules is a problem
Testing of employees' cyber security awareness	Yes	
Reporting of possible cyber-attacks	Barely	
Cyber security professionals should be around for	Yes, but no 24/7 coverage	The IT department is understaffed

consultation and recommendations		

4.5 Commitment to resilience

From the previous sections, it can be concluded that there are a many vulnerabilities concerning the hospital's cyber security. The hospital's network is just too large and complex to be fully secured. Thus, the chance that a security breach occurs is relatively large. This means that the hospital has to be prepared to respond to a security breach. This section analyses the hospital's resilience in this respect. So, what is the ability of the hospital to respond to and recover from breaches in cyber security caused by cyber-attacks? As discussed in the previous chapter, HRO theory values creativity and improvisation over rigidity and anticipation. This section analyses the extent to which these values have been incorporated into the hospital response to and recovery from security breaches.

4.5.1. Differentiating between different kinds of incidents and crises

Despite the fact that an organization has implemented extensive cyber security measures, it is not a question of 'if' a security breach will happen, but 'when' (interview 2, 387-389). Therefore, the hospital has taken out an insurance to cover the damage due to a security breach (Interview 1, 170-172). As discussed previously, there are two kinds of security breaches: discontinuity of operations and violation of privacy. First, a security breach resulting in the discontinuity of operations means that (a part of) the network no longer functions. This could mean that medical data is no longer accessible or that certain medical devices cannot be used anymore. Consequently, the diagnosis and treatment of patients is hindered. Depending on the scale and impact of the breach, the operations of the hospital can potentially come to a standstill which endangers the delivery of patient care (Interview 1, 182-185). Second, a violation of privacy arises when sensitive (patient) information is in the possession of non-authorized actors. This information can both be medical as well as non-medical. Examples of medical information are data on diagnosis and medical treatment. Examples of non-medical information are personal information, for instance name, address and bank account numbers. Since the hospital has a duty to safeguard this information, a leak would constitute a violation of privacy. Not only the information on patients can be leaked, but also the personal information of employees would constitute a violation of privacy.

The impact of a data leak depends on its size. Smaller leaks happen regularly (Interview 2, 441-446). For example, when an email containing sensitive information is sent to the wrong email-

address. Only such a small ‘mistake’ as a typo is needed to make this happen. While this seems to be only a minor violation of privacy, it still has to be reported within 72 hours to the ‘Autoriteit Persoonsgegevens’, which is the Dutch privacy watchdog. Usually such a minor incident is not caused by a security breach, but is due to sloppiness of employees. No extensive damage control is necessary and usually only a short evaluation is sufficient (Interview 2, 462-464). Large-scale data leaks require a more extensive approach. Since such a leak is likely the result of a larger security breach, extensive damage control and a substantial response is required.

The two types of breaches (the discontinuity of operations and the violation of privacy) do not always occur independently from each other. They can occur simultaneously, or one can cause the other. Ransomware is an example of a security breach by which both privacy and the operations are threatened simultaneously. Ransomware is malicious software that encrypts all data on a computer. As a result the user can no longer access his computer (discontinuity of operations). In order to regain access to the computer, the hacker demands a ransom. In return for the ransom, the hacker sends a decryption key. During the hack the hacker likely has accessed files with possible sensitive and personal information (violation of privacy).

An example of one type of breach causing the other type of breach was given by one of the interviewees. This example shows that one crisis, a possible violation of privacy, can cause another crisis, the discontinuity of operations. The radiologist’s home computers are connected to the hospital’s network. When a patient arrives at the emergency department of the hospital in the middle of the night, the radiologist can analyse the scans for home. This speeds up the diagnostic process and allows for a swifter treatment. At some point in time the hospital-CERT received intelligence on vulnerabilities in the encryption of the connection between the radiologist personal home pc’s and the hospital network. The hospital-CERT immediately enabled the external connection because of the risk of violation of privacy. Although the radiologists understood that this was necessary, they did warn about the consequences for patient care; the on call radiologist could no longer analyse the scans from home (discontinuity of operations). The vulnerability had to be patched as quickly as possible (Interview 2 Hospital, 423-439). This example illustrates that cyber security in the hospital is a matter of constant balancing between different interests. On the one hand good patient care, but on the other hand cyber security and privacy.

4.5.2. Responding to a cyber attack

It is important to note that the hospital has not experienced a major cyber crisis (yet), however there have been several close-calls. On the one hand this could be an indication that their preventive and containment measures are effective, on the other hand it can be argued that they have simply been lucky. There is a major cyber crisis when operations come to a standstill due to a cyberattack or when there is a major violation of privacy. The fact that the hospital has not experienced a large cyber crisis yet, means that its intended response to a major crisis has not yet been tested in practice. Thus, the analysis of the hospital response on cyber-attacks can only be based on what the interviewees expects the response to be and based on the content of the contingency plan.

As discussed previously, one typo in an e-mail can already cause a violation of privacy. Potentially such a small incident can eventually lead to a crisis. So, all incidents, even the small ones, are discussed with the affected departments, employees and/or patients. Violations of privacy have to be reported within 72 hours. In this the GDPR, which regulates privacy, is strict. Therefore, the hospital prefers to report every incident; 'better safe than sorry'. The penalties for not reporting are high (Interview 2, 462-464). The hospital-CERT is also responsible for incidents that affect the operations of the hospital. Since these incidents can affect patient care, consultation with medical staff is vital. As already mentioned in section 2.3.4, any organization should have identified what their main assets which are most valuable to an organization. During a cyber incident, protecting these 'crown jewels' should have priority. In case of a hospital it is obvious that the patients are the 'crown jewels'. To allow operations to continue the hospital has certain redundancies and can replace damaged equipment or systems (Interview 1, 186-188). However, not all equipment and systems can easily be replaced. In that case, the effect on the patient care is more immediate. The extent to which improvisation and creativity is used in handling these incidents is hard to determine.

A successful cyber-attack can endanger the continuation of operations and in that way affect patient care. For a large crisis, that stretches the hospital's resources, a general contingency plan exists. When a cyber-attack affects patient care, this plan is put into effect. To manage the crisis, a crisis team is created led by a crisis coordinator. This team is responsible for coordinating the response to the crisis. The crisis coordinator is a member of the medical staff. The reason for this is that while the crisis may have started as a cyber security issue, it now has evolved into a crisis that affects patient care. Difficult decisions about what medical care to prioritize need to be made. Medical staff has the expertise to make these decisions. The hospital-CERT remains

responsible for resolving the cyber security aspect of the crisis. The actions of the hospital-CERT are dictated by what is needed for the continuation of safe patient care. For example, while it could be wise to shut down certain systems, this might harm patient care (Interview 1, 179-185).

To mitigate some of the effects of a successful cyber-attack, certain precautions have been taken, such as back-ups and redundancy. For instance, the hospital has 20 to 30 laptops with back-ups that can be used to allows patient care to continue (Interview 1, 179-200). Depending on the size and impact of the cyber incident, it can be decided to hire external companies specialized in cyber incident response (such as FOX-IT). When hired, these specialized companies will take the lead in responding to the cyber-attack (Interview 3, 664-665; 671-676).

In case of a violation of privacy, it is less likely that the contingency plan needs to be implemented; this type of incident is less likely to interfere with patient care. Therefore, the hospital-CERT has more leeway to respond to these incidents, obviously in consultation with other parties (Interview 2, 411-414). If necessary, external parties can be hired to help in this response (Interview 3, 664-665). As already mentioned before, since the introduction of the GDPR, organizations are required to report data breaches within 72 hours (Interview 2, 462-463). Organizations must report any breach that includes personal information (Article 29 Data Protection Working Party, 2018, p. 7).

Although the interviewees agree that a large scale security breach is going to happen, training the response to cyber incidents does not happen regularly (Interview 1, 202-203). Interviewee 3 argues that it is not possible to properly simulate a real cyber crisis and states that this is as ‘learning to swim, while being out of the water’. However, cyber incidents do occur regularly and this should provide enough material for regular training and testing of the required skills to respond to a security breach (Interview 1, 661-662). The regular penetration testing also can provide enough material for testing and training of the required skills (Interview 2, 417-419). In short, the hospital does not do regular drills on responding to cyber incidents. However, the cyber security team is confident that they can adequately react to most cyber-attacks.

4.5.3 Recovering from a cyber attack

During the response on a cyber crisis, logging all activity occurring during the crisis is important. This allows for analysis on how the cyber-attack could happen and provides valuable information for evaluation of the response. The cyber security team of the hospital stresses the importance of logging and also of other methods of registering what has happened in the

network (Interview 2, 485-489). After the cyber incident, the analysis and evaluation is predominantly the task of the cyber security team. They write the report and implement the 'lessons learned'. Other parties, both internally and externally, that were involved in the incident response contribute to the analysis and evaluation (Interview 3, 467-468).

4.5.4 Conclusion

Two different effects of cyber-attacks can be identified: first, an attack resulting in a violation of privacy and, second, an attack causing a discontinuity in operations. In this it is important to distinguish between small incidents and large crises. As a rule of thumb it can be stated that, the more a cyber-attacks affects patient care, the less authority the hospital-CERT has in addressing the crisis. The main reason for this is that in a hospital, the care for patients (every hospital's 'crown jewels') is always the number one priority. All cyber security measures taken in response to a cyber-attack must be weighed against the effects these measures have on patient care.

In order to be ready for a crisis, the hospital has taken several preparatory measures. Certain redundancies are ready to be allocated in times of needs. Regular back-ups are made, which help in limiting the damage and allows an organization to recover more quickly. However, the hospital is not fully committed to cyber security. There is no additional training and testing of the response to cyber-attacks. The interviewees argue that they do 'train' in an indirect manner for these situations by responding to penetration tests and to smaller incidents. Since the hospital has not yet had to respond to a major cyber incident, it is hard to establishes if the hospital is creative and/or can improvise in their response to such an incident. During an incident, the hospital-CERT extensively logs all actions taken during the response. This allows them do an analysis on its response. Other parties involved in the response are include in the analysis. In short, while certain preparatory measures have been taken to prepare for a major cyber incident, it was not possible to see if these were effective since the hospital has not been involved in a major cyber crisis yet.

Referring to table 2 the extent of the incorporation of the principle of commitment to resilience can be summarized as follows:

Operationalization	**Incorporated?**	**Remarks**
Reserve resources that can be allocated in times of need	Yes	

Daily backups of all systems	Yes	Unclear whether these back-ups are made daily
The crown jewels have been identified	Yes	Patient care is the number one priority
Broad understanding of cyber security among cyber security professionals.	Yes	
Real-time learning and creativity are valued	Could not be established	
Training and testing of cyber resilience	Not sufficient	No official training and testing sessions.
After a cyber incident, assessment of the incident	Yes	
Lessons learned must be implemented	Yes	
A contingency plan that allows for creativity and improvisation	The aspect of creativity and improvisation could not be established	

4.6 Deference to expertise

The HRO theory states that in situations of high stress on an organization individuals with the required expertise should take the lead in responding to a crisis. In this section a distinction is made between either a cyber security breach that does not significantly affect patient care and a cyber security breach which does significantly affect patient care.

4.6.1. A security breach having little or no effect on patient care

In the previous section, the distinction was made between small and large incidents, and cyber-attacks resulting in a violation of privacy or the discontinuation of operations. In general it can be argued that smaller incidents and violations of privacy are less likely to hinder patient care. In these situation, only the hospital-CERT acts. While the CERT does not have formal decision-making power, the board of directors follow their lead in responding to a security breach (Interview 3, 580). However, formally the board of directors is accountable for the actions of the CERT (Interview 2, 470-473). In situations where the effect on patient care is minimal,

there is a clear deference to the expertise of the cyber security specialist. However, this changes when, a cyber-attack does significantly affect patient care.

4.6.2. A security breach having significant effect on patient care

In the case of cyber security incident resulting in a large crisis with discontinuation of operations, is likely to affect patient care. This does not mean that smaller incidents and violations of privacy cannot affect patient care, but this is less likely so. With significant discontinuation of operations, what first was a cyber security incident can evolve into a medical crisis. The escalation is either directly caused by the cyber-attack or indirectly by the response to the cyber-attack. At the time patient care is affected, the hospital-CERT is no longer in the lead. As discussed earlier, in this situation a hospital-wide crisis team is created led by a crisis coordinator. This team coordinates the hospitals response to the crisis (Interview 1, 179-186). The focus is on the continuation of medical care while safeguarding patient safety (Interview 1, 211, Interview 3, 678). All the time the hospital-CERT stays responsible for addressing the cyber security aspect as long as this does not hinder medical care. The CERT coordinates its actions with the medical staff and with the board of directors (Interview 2, 472-473). Since the hospital-CERT has less authority to take his own decision, it can be argued that, from a cyber security perspective, in these situations there is no or limited deference to expertise. However, when a cyber security crisis has evolved into a medical crisis, deference to medical expertise is the right step to take. As the crisis has evolved, the deference to expertise has evolved too. Since a large crisis put large amounts of stress on an organization, it might be necessary to hire external help and expertise. There are multiple companies specialized in cyber security crisis response. The can deliver the required cyber expertise (Interview 3, 665-669). It is clear that, because of the prioritization of patient care, also these organizations have to coordinate their actions with the medical staff and the board of directors.

4.6.3 Conclusion

The deference to expertise depends on the extent to which patient care is affected as result of the cyber-attack or the response to the cyber-attack. The rule of thumb is: the more patient care is affected by a cyber-attack, the less deference to only cyber security expertise and the more deference to mainly medical expertise. Thus from a pure cyber security perspective, there is no complete deference to expertise. The hospital-CERT can only act in coordination with other actors. Although they are responsible for responding to the cyber aspect of their crisis, their actions must weighed against the effects on patient care.

Referring to table 2 the extent of the incorporation of the principle of deference to expertise can be summarized as follows:

Operationalization	**Incorporated?**	**Remarks**
During cyber-attacks, most qualified person gains decision-making power	Depends on the extent to which patient care is affected	
If expertise is missing, external expertise is brought in	Yes	

4.7 Answering the research question

This chapter has analysed the incorporation of the principles of HRO theory in the hospital's approach to cyber security. The findings of this chapter are summarized in table 3.

Operationalization	**Incorporated?**	**Remarks**
<u>Preoccupation with failure</u>		
Reward for the reporting of errors, vulnerabilities and anomalies, no punishments	No	
Open discussion of problems	Not obvious	
Close-calls are carefully analysed to find vulnerabilities	Yes,	Only the most urgent close-calls are analysed (and patched if necessary)
A CVD program exists	Yes, but not well known	Even in the IT department itself not everyone knew that it existed
Yearly penetration testing or after significant changes to a system	Yes	
The detection of irregularities and anomalies through a SOC	Yes	
<u>Reluctance to simplify interpretations</u>		
Constant questioning of assumptions is encouraged	Not obvious	

Diverse team, consisting both out of cyber security experts and ‘normal’ employees	No	The CERT consists only of IT-experts
Extensive analysis of every cyber incident	No	The workload of the CERT is too high
<u>Sensitivity to operations</u>		
Clear picture of the main threats	Yes and no	Intelligence gathering from multiple sources, but insufficient resources for good analysis
Sharing threat intelligence	Yes	
Cyber security awareness training for all employees	Minimal	
Basic cyber security rules for all employees	Yes	Adherence to these rules is a problem
Testing of employees’ cyber security awareness	Yes	
Reporting of possible cyber-attacks	Barely	
Cyber security professionals should be around for consultation and recommendations	Yes, but no 24/7 coverage	The IT department is understaffed
<u>Commitment to resilience</u>		
Reserve resources that can be allocated in times of need	Yes	

Daily backups of all systems	Yes	Unclear whether these back-ups are made daily
The crown jewels have been identified	Yes	Patient care is the number one priority
Broad understanding of cyber security among cyber security professionals.	Yes	
Real-time learning and creativity are valued	Could not be established	
Training and testing of cyber resilience	Not sufficient	No official training and testing sessions.
After a cyber incident, assessment of the incident	Yes	
Lessons learned must be implemented	Yes	
A contingency plan that allows for creativity and improvisation	The aspect of creativity and improvisation could not be established	
<u>Deference to expertise</u>		
During cyber-attacks, most qualified person gains decision-making power	Depends on the extent to which patient care is affected	
If expertise is missing, external expertise is brought in	Yes	

Table 3. Overview of the incorporation of HRO theory in the hospital's cyber security

The research question of this this thesis is: *To what extent have the ideas derived from High Reliability Organizations been incorporated in organizations concerned with cyber security, and how can discrepancies be explained?* As the table above shows, the answer to the first part of this question (*´To what extent have the ideas derived from High Reliability Organizations been incorporated in organizations concerned with cyber security?')* is that none of the organizing HRO principles have been fully incorporated in the hospital's approach to cyber security. First, 'the preoccupation of failure' has been partly incorporated by partnering with external parties for the identification of vulnerabilities and detection of anomalies. However,

internally the incorporation of ‘the preoccupation with failure’ has not been fulfilled. As a result of this, employees rarely report issues. Also, there is no indication that incidents and problems are openly discussed, which helps in identifying and detecting errors. Second, full incorporation of ‘the reluctance to simplify interpretations’ has not accomplished either. The workload of the hospital-CERT is too high to fully analyse each incident and error; they have insufficient time and resources. Furthermore, the quality of the analysis made by the hospital-CERT might improve by expanding the team and by allowing more diversity in expertise within the hospital-CERT. Third, ‘the sensitivity to operations’ has been incorporated to the extent that the hospital-CERT is aware of, and understands, the main threats as far as is possible. Extensive networks exist for the sharing and gathering of threat intelligence. However, there seems to be little sensitivity to operations among employees. Most employees have insufficient cyber security awareness. This leaves the hospital extremely vulnerable. Fourth, ‘the commitment to resilience’ has been incorporated to the extent that several preparatory steps have been taken. However, there is little information about the incorporation of values such as creativity and improvisation in the response to security breaches. Fifth, depending on the circumstances, the ‘deference to expertise’ seems to have been mostly incorporated. The extent of the incorporation depends on the extent to which patient care is affected by a security beach. In general, the more patient care is affected, the less deference to cyber expertise only.

In conclusion, the principles of HRO theory have not been fully incorporated in the hospital, which answers the first part of the research question. Now, the second part of the research question needs to be answered: *‘how can discrepancies be explained?’*. From table 3, and form the discussions in the previous sections, it can be derived that there are two main findings that can explain for the discrepancies;

1. <u>Failure to prioritize cyber security in the hospital</u>

   Taking care of patients is the main priority of the hospital, not cyber security. Although this is understandable, this can lead to underestimating the importance of cyber security. Not prioritizing cyber security can lead to ‘poor’ cyber security which enhances the risk of a security breach; this in turn directly threatens patient care. Since the hospital fails to sufficiently prioritize cyber security, insufficient resources are allocated to cyber security. This results in, amongst others, an overworked hospital-CERT and minimal training and testing which further weakens the hospital’s cyber security. Although the prioritization of patient care is sensible from a medical perspective, it is problematic from a cyber security perspective. It is not argued that cyber security should be valued over medical care, but

cyber security should be of equal importance or at least a close second priority. The failure to prioritize cyber security prevents the full incorporation of the principles of HRO theory in the hospital. This is in line with the criticism of Levenson et al. (2009, pp. 237-241, discussed in section 2.2.1); HRO theory might be more difficult to implement in organizations whose primary goals are not safety or reliability.

2. Low level of awareness among employees

   The majority of employees are unaware of the importance of cyber security. This lack of awareness prevents the full incorporation of HRO principles as 'preoccupation with failure', 'reluctance to simplify interpretations' and 'sensitivity to operations'. Since the employees do not understand the importance of cyber security, they barely reports any suspicious circumstances and form a weak link in the hospital's cyber security. Thus, there is an urgent need for improvement of awareness and understanding of cyber security. Without this, the hospital's security remains at risk.

Chapter 5: Discussion & Reflection

Today's world is quickly digitalizing. Society increasingly relies on digital technology. Not only our daily lives become more digitalized, but also critical infrastructures increasingly relies on digital technology. Even though this digitalization has brought us many good, it has also comes with new risks. To protect ourselves, all digital systems and networks need to be cyber secure. However, creating this security is an enormous challenge. This thesis aims to contribute to our understanding of the creation of cyber security, by analysing the extent to which HRO theory has been incorporated in an entity's cyber security. The research question is formulated as follows: '*To what extent have the ideas derived from High Reliability Organizations been incorporated in organizations concerned with cyber security, and how can discrepancies be explained?'*

To be able to answer the research question first a theoretical framework was created (chapter 2). This framework shows that, from a theoretical perspective, it is possible to 'translate' the principles of HRO theory to the NIST framework, on which this thesis' definition of cyber security is based. Applying the principles of HRO theory is adding to our understanding of cyber security especially when it comes to its human and organizational aspects. However, 'in theory there is no difference between theory and practice – in practice there is' (Quoteresearch, 2018). Thus, it is necessary to go from theory to practice. Chapter 3 describes the methodology of case study design to find an answer to the research question. In chapter 4, the theoretical framework was tested by the analysis of a hospital's cyber security. This analysis shows that the principles from HRO theory have not been fully incorporated in the hospital's cyber security approach. The extent to which each of the HRO principles have been incorporated is presented in table 3. From this table it can be derived that there are roughly two main findings that explain discrepancies in the incorporation of the principles of HRO theory in the hospital's cyber security: the non-prioritization of cyber security and the low level of cyber security awareness among employees.

The findings of this thesis underline the differences between organizations that have successfully fully incorporated HRO theory in their cyber security, such as the US Defense Department, and an organization that have not, such as the hospital in this case study. In the US Defense Department there is organization-wide realization that cyber security is more than a IT issue; the role of human conduct in cyber security is recognized and taken in account. The whole organization needs to apply the organizing principals of HRO theory to make it work

(Winnefeld Jr., Kirchhoff, & Upton, 2015). So, the whole organization must realize that cyber security is a serious problem and must be willing to address this problem. In the hospital there is, in general, insufficient realization of the importance of cyber security. Cyber security needs to be more prioritized and the directors of the hospital need to be made aware of this. Prioritizing cyber security starts with providing the hospital-CERT, and the IT department, with sufficient manpower and resources to allow them to fully analyze every close-call to find vulnerabilities. Furthermore all employees in the hospital must realize that cyber security is a serious issue that requires serious attention; it is not something you do at the side. This awareness can be created by the rewarding of reporting of vulnerabilities and cyber awareness training for all employees. Creating the necessary awareness is further discussed in section 5.2. When the awareness has been created, the organization and its employees must be provided with clear guidelines on what good cyber security involves. Adherence to these guidelines must be continuously tested.

Recent publications in newspapers provide evidence that the hospital in the case study is not the only hospital that faces cyber security challenges. All organizations have to realize that cyber security is more than only a challenge for the IT department and that the human conduct play a pivotal role in this. The principles of HRO theory can provide a guidance on what is needed to create the necessary cyber security mindset and what potential barriers need to be overcome.

5.1. Limitations and recommendations for future research

As all research, this thesis has certain limitations. The recommendations for future research are based on these limitations. The first limitation of this research is that this thesis only consists of one case study. Hence, one must be careful in generalizing the findings of this thesis. For generalization purposes it is recommended to do more case studies in different types of organizations on the extent of the incorporation of the principles of HRO theory in their approach to cyber security.

The second limitation of this research is that the hospital has not (yet) gone through a major crisis as the result of cyber-attack. Therefore, the analysis of the ‘commitment to resilience’ and ‘deference to expertise’ is partly based on what the interviewees expect to do in such a situation. This can differ from what they actually would do during a crisis. Since crises often pan out differently than expected, the expectations of the interviewees might not hold up. Thus, the sections on ‘the commitment to resilience’ and ‘deference to expertise’ have a more hypothetical character. It is recommended that future research should focus on case studies of

organizations that have gone through a major cyber crisis. It would be ideal if an researcher could observe how an organization is responding to, and recover from, during a cyber-attack. However, it is unlikely that a researcher is in place during the early stages of the crisis response. Good alternatives are observations during the testing and training of the response or interviewing the actors afterwards.

The third limitation is the fact that major parts of the hospital's cyber security have been outsourced. The hospital relies heavily on external suppliers of specialized cyber security products and services. Examples are the firewall, penetration testing and the SOC. Contrary to an organization such as a hospital, it is obvious that these external suppliers do prioritize cyber security as being their core business. This thesis has not analyzed the extent of incorporation of principles of HRO theory in these external suppliers. Future research should analyze to what extent principles of HRO theory has been incorporated in these external suppliers and, if this can compensate for the finding that principles of HRO theory are not fully 'internally' incorporated in an organization.

5.2. Recommendations for the hospital (and for the medical sector)

As discussed there are roughly two main findings that explain discrepancies in the incorporation of the principles of HRO theory in the hospital's cyber security: the non-prioritization of cyber security and the low level of cyber security awareness among employees. So, recommendations must focus on these two findings. These recommendations are specific for the hospital in the case study but might also be valid for the medical sector as a whole.

As already mentioned it all start with prioritizing cyber security and making the directors of the hospital aware of this. Making manpower and sufficient resources available to the hospital-CERT, and the IT department, is needed to improve the awareness and understanding of cyber security amongst employees. A long term awareness strategy needs to be designed. Bauer et al (2017) have identified certain characteristics that make an awareness program effective. First, the material used in the training should be comprised of a mix of sources. A combination of different training methods and tools should be used. For example, the strategy should not just consists of an e-learning course, but of a mix of e-learning, quizzes, testing and other methods. This diversification improves the effectiveness of awareness training. Second, the strategy needs to be long-term. Cyber security is a constant process that never stops. The same thinking applies to the awareness strategy. The training and testing of awareness needs to regularly repeated in a continuous process. For an effective strategy, evaluation of the strategy and

methods used is key. If it is learned that a method or training is ineffective, there should flexibility to update the strategy. Third, good communication is key. Most employees do not have a technical background and possess minimal knowledge of cyber security. The use of jargon and abbreviation can greatly hinder an employees' understanding of awareness and cyber security. The communication should be understandable for all employees. Fourth, one must differentiate between target audiences. People have different personalities. Some methods are more effective in influencing certain personalities than others. The specific targeting of personality groups can improves awareness and compliance to cyber security (Bauer, Bernroider, & Chudzikowski, 2017, pp. 152-154).

The second recommendation for the hospital is to diversify the team responsible for cyber security. Currently, all member of the hospital-CERT have an IT background. Since cyber security and patient care are closely linked together in the hospital, the hospital-CERT should duplicate this link by including medical professionals. This allows for multiple perspectives on the problems which results in a better understanding.

The third recommendation is to train for large security breaches. Since all interviewees agreed that a security breach is going to happen someday, training for these situations is crucial. By simulating a crisis, it can be learned how people behave under pressure and in what areas of the response and recovery there is need for improvement.

Bibliography

AD. (2018, April 26). *Liefst 85 ziekenhuismedewerkers bestraft voor neuzen in dossier Barbie*. Opgehaald van AD: https://www.ad.nl/binnenland/liefst-85-ziekenhuismedewerkers-bestraft-voor-neuzen-in-dossier-barbie~aedceabe/

Article 29 Data Protection Working Party. (2018, February 6). *Guidelines on Personal data breach notification under Regulation 2016/679.* Opgehaald van European Commission: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

Austrlian Associated Press. (2019, October 1). *Systems shut down in Victorian hospitals after suspected cyber attack*. Opgehaald van The Guardian: https://www.theguardian.com/australia-news/2019/oct/01/systems-shut-down-in-victorian-hospitals-after-suspected-cyber-attack

Bagnara, S., Parlangeli, O., & Tartaglia, R. (2010). Are hospitals becoming high reliability organizations? *Applied Ergonomics, 41*, 713-718.

Barnett, R., Cornell, D., Hoffman, A., & Knobloch, M. (sd). *Virtual Patching Best Practices*. Opgehaald van OWASP: https://owasp.org/www-community/Virtual_Patching_Best_Practices

Barrett, M. P. (2018, April 16). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1* . Opgehaald van National Institute for Standards and Technology: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

Batteau, A. W. (2011). Creating a Culture of Enterprise Cybersecurity. *International Journal of Business Anthropology, 2*(2), 36-47.

Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security, 68*, 145-159.

Burns, A. (2019). Security Organizing: A Framework for Organizational Information Security Mindfulness. *The DATA BASE for Advances in Information Systems, 50*(4), 14-27.

Choi, S. J., Johnson, M. E., & Lehmann, C. U. (2019). Data breach remediation efforts and their implications for hospital quality. *Health Services Research, 54*(5), 971-980.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014, October). Defining Cybersecurity. *Technology Innovation Management Review*, 13-21.

De Crespigny, M. (2012). Building cyber-resilience to tackle threats. *Network Security, 4*, 5-8.

De IT-Auditor. (2015, March 30). *Cybersecurityrisico's medische apparatuur*. Opgehaald van De IT-Auditor: https://www.deitauditor.nl/informatiebeveiliging/cybersecurityrisicos-medische-apparatuur/

Dixon, N. M., & Shofer, M. (2006). Struggling to Invent High-Reliability Organizations in Health Care Settings: Insights from the Field. *Healt Service Research, 41*(4), 1618-1632.

Donaldson, S. (2014, March 17). *Virtual Patching is what, exactly?* Opgehaald van Bitdefender: https://businessinsights.bitdefender.com/what-is-virtual-patching

ENISA 1. (sd). *Glossary*. Opgehaald van European Union Agency for Cyber Security: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary#G52

Fire Eye. (2019). *M-Trends.* Opgehaald van https://content.fireeye.com/m-trends/rpt-m-trends-2019

Forescout. (2019). *Putting Healthcare Security Under the Microscope.* San Jose: Forescout Technologies inc.

GAO. (2012, August 31). *Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices.* Opgehaald van U.S. Government Accountability Office: https://www.gao.gov/products/GAO-12-816

Gillham, B. (2005). *Research Interviewing: The Range of Techniques.* Maidenhead: Open University Press.

Graham, C. (2017, May 20). *NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history*. Opgehaald van The Telegraph: https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/

Kapersky. (sd). *The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within*. Opgehaald van Kapersky: https://www.kaspersky.com/blog/the-human-factor-in-it-security/

KPMG. (2013). *Vijf denkfouten over cybersecurity: Een bestuurdersperspectief op Cyber Security.* Opgehaald van Beveligingswereld.nl: http://www.beveiligingswereld.nl/files/KPMG-Vijf-denkfouten-over-cybersecurity.pdf

La Porte, T. R. (1996). High Reliability Organizations: Unlikely Demanding and at risk. *Journal of Contingencies and Crisis Management*, 60-71.

LaPorte, T., & Consolini, P. M. (1991). Working in Practice but Not in Theory: Theoretical Challenges of "High-Reliability Organizations". *Journal of Public Administration Research and Theory: J-PART*, 19-48.

Levenson, N., Dulac, N., Marais, K., & Carroll, J. (2009). Moving Beyond Normal Accidents and High Reliability Organizations: A Systems Approach to Safety in Complex Systems. *Organization Studies, 30*(2&3), 227-249.

Metz, L. (2017). *The Definitive Guide to Sharing Threat Intelligence.* Opgehaald van The Hague Security Delta: https://www.thehaguesecuritydelta.com/media/com_hsd/report/159/document/The-Definitive-Guide-to-Sharing-Threat-Intelligence.pdf

NCSC. (2017, September 20). *Factsheet SOC inrichten: begin klein.* Opgehaald van Natiionaal Cyber Security Centrum: https://www.ncsc.nl/aan-de-slag/documenten/factsheets/2019/juni/01/soc-inrichten

NCSC. (2017, August 8). *Pentration Testing*. Opgehaald van National Cyber Security Centre: https://www.ncsc.gov.uk/guidance/penetration-testing

NCSC. (2018, October 2). *Leidraad Coordinated Vulnerability Disclosure.* Opgehaald van Nationaal Cyber Security Centrum: https://www.ncsc.nl/aan-de-slag/documenten/publicaties/2019/mei/01/cvd-leidraad

NCTV. (2019, June 12). *Cybersecuritybeeld Nederland 2019.* Opgehaald van Nationaal Coördinator Terrorismebestrijdeing en Veiligheid: https://www.nctv.nl/documenten/publicaties/2019/6/12/cybersecuritybeeld-nederland-2019

NIST. (2012, September 17). *Guide for Conducting Risk Assessments.* Opgehaald van National Institute for Standards and Technology: https://www.nist.gov/publications/guide-conducting-risk-assessments

NOS. (2018, January 2018). *Speciaal team gaat ziekenhuizen helpen bij cyberaanval*. Opgehaald van NOS: https://nos.nl/artikel/2213485-speciaal-team-gaat-ziekenhuizen-helpen-bij-cyberaanval.html

Perrow, C. (1984). *Normal Accidetns: Living with HIgh-Risk Technologies.* Princeton, New Jersey: Princeton University Press.

Quoteresearch. (2018, April 14). *In Theory There Is No Difference Between Theory and Practice, While In Practice There Is*. Opgehaald van Quote Investigator: https://quoteinvestigator.com/2018/04/14/theory/#note-18386-6

Robert, K. H., Madsen, P., Desai, V., & Van Stralen, D. (2005). A case of the birth and death of a high reliability healthcareorganisation. *Quality and Safety in Health Care, 14*(3), 216-220.

Rochlin, G. I. (1996). Reliable Organizations: Present Research and Future Directions. *Journal of Contingencies and Crisis Management, 4*(2), 55-59.

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2019, September 16). *Developing Cyber Resilient Systems: A Systems Security Engineering Approach.* Opgehaald van National Institute of Standards and Technology: https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/draft

Rumsfeld, D. (2002, February 12). *DoD News Briefing - Secretary Rumsfeld and Gen. Myers*. Opgehaald van U.S. Department of Defense: https://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636

Samarati, M. (2017, January 12). *How often should I schedule a penetration test?* Opgehaald van IT Governance: https://www.itgovernance.co.uk/blog/how-often-should-i-schedule-a-penetration-test

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law, 12*(2), 53-74.

Schippers, E. (2016, July 6). *Antwoorden op kamervragen van de Kamerleden Verhoeven (D66) en Dijkstra (D66) over het bericht 'Cyber security van apparatuur in*

ziekenhuizen kwetsbaar'. Opgehaald van Rijksoverheid: Antwoorden op kamervragen van de Kamerleden Verhoeven (D66) en Dijkstra (D66) over het bericht 'Cyber security van apparatuur in ziekenhuizen kwetsbaar'.

Schofield, J. (2008, Februari 14). *Never assume your data is safe, even if it's online* . Opgehaald van The Guardian: https://www.theguardian.com/technology/2008/feb/14/email.yahoo

Schulman, P. R. (1993). The negotiated order of organizational reliability. *Administration & Society, 25*(3), 353-372.

Shawn Burke, C., Wilson, K. A., & Salas, E. (2005). The use of a team-based strategy for organizational transformation: guidance for moving toward a high reliability organization. *Theoretical Issues in Ergonomics Science, 6*(6), 509-530.

Weick, K. E., & Roberts, K. H. (1993). Collective mind in organizations: Heedful interrelating on flight decks. *Administrative Science Quarterly, 38*(3), 357-381.

Weick, K. E., & Sutcliffe, K. M. (2007). *Managing the Unexpected: Resilient Performance in an Age of Uncertainty.* San Fransisco: Josey-Bass.

Wilson, M., & Hash, J. (2003, October). *Building an Information Technology Security Awareness and Training Program.* Opgehaald van National Institute of Standards and Technology: https://csrc.nist.gov/publications/detail/sp/800-50/final

Winnefeld Jr., J. A., Kirchhoff, C., & Upton, D. M. (2015, September). Cybersecurity's Human Factor: Lessons from the Pentagon. *Harvard Business Review*, 86-95.

Yin, R. K. (2009). *Case Study Research: Design and Methods.* Thousand Oaks: Sage.

Z-CERT. (sd). *Organisatie*. Opgehaald van Z-CERT: Computer Emergency Response Team voor de zorg: https://www.z-cert.nl/over-z-cert

Zerlang, J. (2017, June). GDPR: a milestone in convergence for cyber-security and compliance. *Network Security, 6*, 8-11.

Zohar, D., & Luria, G. (2003). Organizational meta-scripts as a source of high reliability: the case of an army armored brigade. *Journal of Organizational Behavior, 24*, 837-859.

Annex: Interviews Hospital

Legend:

- Preoccupation with failure
- Reluctance to simplify
- Sensitivity to operations
- Commitment to resilience
- Deference to expertise

Interview 1 Hospital: Manager Computerization & Automation

Hoe wordt er in uw organisatie gezocht naar zwakheden/vulnerabilities?

Dit word gedaan uit verschillende perspectieven. Het ICT perspectief is wat het dichts bij ons staat. Sowieso hebben we beleid opgesteld. Dit doen we samen met de raad van bestuur en met de medische staf. Wij proberen gewoon te voorkomen dat we hier problemen krijgen met security. Tot nu toe is dat ook nog gelukt, er is nog niet iets vervelends gebeurd in dit ziekenhuis.

We zijn continu bezig om ons te informeren via allerlei gremia, via de NVZ, de Nederlandse Vereniging voor Ziekenhuizen, die hebben een overleg speciaal voor security officers. Je hebt zorg-CERT. Je hebt allerlei gremia waarbij wij zijn aangesloten en waardoor we proberen alle ontwikkelingen op de voet te volgen.

We hebben dus een Chief Information Security Officer (CISO), wiens enige taak is om zorgen dat het ziekenhuis, qua informatiebeveiliging veilig is. Hij heeft er veel verstand, want hij komt uit de ICT, zoals systeembeheer enzovoorts. Dus ik denk dat we wat dat betreft heel goed weten wat voor soort ontwikkelingen er zijn. We laten ons graag ook informeren door leveranciers vanuit de markt en een deel van onze informatiebeveiliging besteden we ook uit. Dit doen we vooral daar waar we het niet zelf kunnen.

Wordt er veel uitbesteed? Ik kan me namelijk voorstellen dat cyber security steeds ingewikkelder wordt.

Als we het hebben over een nieuwe firewall bijvoorbeeld, dan doen we dat samen met echte experts in de markt. We gaan dan in discussie met de leveranciers.

Af en toe besteden we een dienst uit, bijvoorbeeld een dienst die ons netwerk monitort. Ons netwerk wordt 24/7 gemonitord. Op het moment zij iets raars zien, worden wij opgebeld en nemen we een kijkje.

En als zij iets raars vinden, zeggen zij van "kijk hier even naar"?

Ja precies

Dus zowel intern als extern wordt er gekeken naar "rare" dingen?

Ja, we doen bijvoorbeeld ook pen testen.

Omdat we een eigen patiënten portaal hebben, moeten we een Digi-D audit doen. De reden hiervoor is dat je met Digi-D inlogt in het patiënten portaal. De eisen voor de Digi-D audit worden met de dag strenger. Dus ja dat betekent ook dat we ook op dat vlak veel aandacht moeten besteden aan informatie veiligheid.

Hebben jullie dan ook een CVD programma? Dat is een Coordinated Vulnerability Disclosure programma, waar mensen gaan zoeken naar zwakheden in een systeem. Als ze een zwakheid vinden en die melden, dan krijgen ze vaak een bepaalde beloning, bijvoorbeeld een geldbedrag.

Nee dat hebben we niet. Daar huren we gewoon externe partijen voor in. Zij proberen ons te hacken. Ook laten we onze beleidsdocumenten analyseren, een soort van paper reviews. En we hebben volgens mij een bepaalde policy dat als mensen, bijvoorbeeld patiënten, op het gebied van informatie beveiliging iets vinden dan moeten ze dat aan ons melden. Wij moeten dan binnen 72 uur actie ondernemen. Als wij dit niet doen, dan mag die persoon naar de pers gaan.

Geldt hetzelfde ook als een werknemer iets vindt, moeten die dit dan ook melden?

Daar hebben wij allerlei systemen voor. Als een medewerker iets vindt op het gebied van informatiebeveiliging hebben we daar een meldingssysteem voor. We hebben een meldingssysteem voor incidenten met patiënten, maar onderdeel van hetzelfde systeem is dat ze IT dingen kunnen melden.

Wordt dit systeem ook vaak gebruikt?

Nee, ik heb tot nu toe vooral gehad over de ICT component, maar het grootste probleem zijn de medewerkers. Maar ook daar zijn we druk bezig om mensen te informeren over wat ze

moeten doen. Als je op de ziekenhuis website kijkt zie je eens in de zoveel tijd een cartoon met een vraag. Maar we hebben ook een externe bedrijven die af en toe een spam bericht op het netwerk zetten. We kijken dan hoe de medewerkers hierop reageren.

Wat gebeurt er tijdens zogenaamde close calls, dat het maar net goed ging?

Er zijn in het verleden wel is wat close calls geweest met virusscanners. Het probleem met een ziekenhuis is dat de ICT apparatuur prima is. Er draaien allerlei virusscanners om heen, verschillende lagen zelfs. Als je kijkt naar de medische apparatuur, is dat een kwetsbaar punt voor alle ziekenhuizen. Medische apparatuur draait vaak op verouderde software, soms zelfs nog op Windows XP. Binnenkort zullen we problemen krijgen met dingen die nog op Windows 7 draaien. De fabrikanten van die apparatuur zeggen dat je er geen virusscanner op mag draaien want dan gaat de performance van het apparaat omlaag. Daar zitten zeker nog wat vulnerabilities, maar dat geldt voor alle ziekenhuizen. Daar zou meer aandacht aan besteed moeten worden.

Dus eigenlijk is het netwerk van het ziekenhuis zelf wel goed beveiligd, in ieder geval zo ver je kan beveiligen, maar de meeste apparaten die gebruikte worden, daar zitten risico's.

Daar zijn de risico's aanzienlijk groter dan bij pure ict apparatuur.

Het team dat zich bezighoudt met cyber security, uit hoe veel mensen bestaat dat?

Daar zijn verschillende mensen mee bezig. De CISO is daar fulltime mee bezig. Binnen het team van systeembeheer zijn er toch wel twee à drie mensen veel mee bezig. Qua fte weet ik het niet precies. Maar je merkt gewoon dat er een steeds groter deel van onze tijd moeten besteden aan informatie beveiliging. Als je alleen maar kijkt naar die Digi-D audit, die we moeten doen voor het patiënten portaal. Dat kost ons gewoon maanden voorbereidingstijd.

Wat is dat precies die Digi-D audit?

Bij ons patiënten portaal maken wij gebruik van Digi-D als inlogmechanisme, dat doet bijna ieder ziekenhuis. Om gebruik te mogen maken van Digi-D moet je ieder jaar geaudit worden. Je moet pen testen doen. Het is een heel circus dat ieder jaar zwaarder wordt. Daar zijn we met projectleiders, ict experts en de CISO vijf maanden bezig om dat op de rit te krijgen, ieder jaar weer.

Dat soort dingen zorgen er dus voor dat het erg veel tijd kost.

Ja, maar daarmee krijgen we als bijvangst dat we ook allerlei anderen vulnerabilities in het netwerk vinden.

Want als er geen Digi-D audit zou zijn geweest, zouden jullie dit allemaal zelf moeten doen.

Wij doen het nu gedwongen die Digi-D audit, want anders kunnen wij het patiënten portaal niet in de lucht houden. Normaliter doen wij al heel veel dingen uit ons zelf. Ook willen wij NEN 7510 gecertificeerd zijn aan het einde van dit jaar. Daar is de CISO ook mee bezig. Dus dat is ook alweer informatiebeveiliging. We willen laten zien, ook aan de patiënten, dat hun gegevens hier veilig zijn en dat we alles goed voor elkaar hebben.

Er zijn constant nieuwe dreigingen. Hoe zorgt u ervoor dat u up-to-date blijft, dat u weet wat er speelt?

We hebben nu bijvoorbeeld een zorg-CERT. Die mensen letten op wat er gebeurt. Als er iets raars aan de hand is worden we daarover geïnformeerd. Onze virusscanners worden minstens dagelijks geüpdatet. Je hebt altijd zero-day exploits. Ik kan niet garanderen dat wij dat nooit zullen hebben, maar de kans is niet zo heel erg groot.

Wat denkt u dat de grootste dreiging is voor de cyber security is in uw ziekenhuis?

De medewerkers zijn het grootste risico. Initieel was het zo dat onze CISO vaak door het gebouw ging lopen om te kijken wat hij allemaal kon vinden, bijvoorbeeld PC's die open staan met patiëntgegevens. Maar nu hebben een recherchebureau ingehuurd om te kijken, met social engineering enzo, of ze kunnen binnendringen op ons netwerk. Het resultaat heb ik net binnengekregen. Medewerkers zijn wel een beetje aan het kijken van wat doet die meneer hier, maar ze krijgen wel de gelegenheid om zomaar achter een pc te gaan zitten. Daar kunnen ze dan allerlei apparatuur aan hangen. Ze hebben gemerkt dat het bijna onmogelijk is om op ons netwerk te komen. Dus dat hebben we wel goed geregeld. Echter komen ze wel overal binnen. Er is er zelfs één die is uitgenodigd om tijdens een OK sessie te komen te kijken. Hij was binnengedrongen in het OK complex en deed net alsof hij nieuw was. Door te zeggen dat hij de opdracht had gekregen om mee te kijken bij een operatie, slaagde hij erin binnen te komen. Dus ook daar proberen we goed te kijken waar zitten onze vulnerabilities.

Hoe kan je zorgen dat je normale werknemers voorbereid zijn op zulke incidenten?

Zoals ik al zei, we doen van die spam berichten. Als mensen daar dan intuinen dan krijgen ze een bepaalde boodschap van "dit is niet goed'. Ook moeten ze dan een bepaalde e-learning

cursus volgen. Maar ook de resultaten van dit onderzoek moeten we publiceren op de een of andere manier. Dat begint bij het management. Zij moeten ervan bewust zijn, maar ook de medewerkers moeten zich bewust zijn van de risico's. Dit is gewoon erg lastig

Dit hoor en lees je inderdaad dat gewoon erg lastig is.

Er is ook zo'n affaire gehad in het Haga ziekenhuis, de Barbie-affaire. Na de Barbie-affaire hadden ze nog een akkefietje waarbij een medewerker een boodschappenlijstje had gemaakt op de achterkant van een papiertje waar patiëntgegevens opstonden. Dat papiertje is toen in het boodschappen mandje blijven liggen en gevonden door iemand anders. Doordat zij nu twee keer zijn "gepakt", zie je dat er allerlei autoriteiten op af komen. Vervolgens moeten ze het netwerk volledig dichtschroeven, waardoor iedereen volledig gefrustreerd is en ze amper meer aan werken toekomen. Wij proberen continu de gulden middenweg te vinden. Het moet veilig zijn, maar ook werkbaar blijven.

U zei net al dat als medewerkers iets verdacht zijn, ze dat kunnen melden. Hoe werkt dit precies?

Daar hebben we een systeem voor. Je kunt hier VIM meldingen doen, Veiligheid en Incident Meldingen. Je kunt bijvoorbeeld een melding als je je onheus bejegend voelt door een andere medewerker. Dit kan gevaar opleveren voor een patiënt. Ook kunnen informatie beveiligingsmeldingen worden gedaan.

Is een beveiligingslek mogelijk bij het ziekenhuis?

Ja, de kans dat het gebeurt is 100%. De vraag is dan wanneer het gebeurt. Wij moeten datalekken ook melden bij de autoriteit, maar we doen eerst zelf beoordeling. Maar een datalek kan al zijn dat er een papiertje uit de printer komt en dat daar dan een tijdje ligt. Het is onmogelijk om het helemaal dicht te timmeren. Het gaat gebeuren.

Komen die datalekken regelmatig voor?

We hadden laatst, dat was echt een datalek, dat iemand een mailtje stuurde met een vraag om bepaalde medische gegevens te leveren. Dat is een regulier procedure. We hebben een reply op die mail gegeven. Maar ergens in de service van de provider was iets raars, want de reply was gestuurd naar het email adres, maar ook naar een ander emailadres dat verbonden was met het originele emailadres. Dus die medisch gegevens kwamen ergens ander terecht. In dit geval hadden we alle procedures goed doorlopen, maar door er ergens iets net niet goed zat, was dit toch een datalek. Eigenlijk is mail niet meer veilig. Als je het juiste emailadres hebt, is

het wel veilig. De manier van versturen is wel veilig, maar als je het naar het verkeerde emailadres verstuurt, en die kans is best groot, heb je een probleem. Dus wat wij nu liever doen is het niet meer versturen van medische gegevens via email naar patiënten, maar soms moeten we wel. In plaats daarvan doen wij dit via het patiënten portaal. Hier loggen zij op in door middel van Digi-D en op dit moment is Digi-D nog veilig genoeg.

Digi-D kan ook niet 100% veilig zijn, maar het is dus wel beter dan email

Inderdaad, Digi-D staat ook niet bekend als het allerhoogste veiligheidsniveau.

Hoe zou het wel allerhoogste veiligheidsniveau kunnen hebben?

Ik geloof dat je Digi-D wat veiliger kan maken doordat je jezelf op de een of andere manier certificeert. Dat kan ook met een nieuwere IPhone. Hier kan je je Digi-D app op de een of andere manier certificeren, dus koppelen aan je identiteit. Ik weet niet precies hoe het gaat maar hierdoor ben je weer een graadje veiliger. Zo zijn er continu ontwikkelingen.

Kunt u zich voorbereiden op zo'n datalek?

Ik heb je nu een voorbeeld gegeven van een lek, maar voor het gevoel zijn het lekjes. Er kan ook wel eens een heel groot lek ontstaan. Dan heb je dus een groot probleem. Bijvoorbeeld een tijd terug in het ziekenhuis in Gouda hebben ze dat gehad. Daar hadden ze een server met verouderde patiëntgegevens in de cloud staan en die was bereikbaar met een heel simpel netwerk. Dat was gekraakt en dus kwamen de autoriteiten weer op bezoek. En dan krijg je dus een heel gedoe, want binnen een maand ben je gewoon een miljoen euro kwijt aan het inhuren van allerlei bureaus die je gaan helpen om te achterhalen wat er gebeurt is en om te proberen de schuldige te pakken. Wij hebben daar trouwens een verzekering voor afgesloten. Maar je wilt dat niet, want binnen een dag, is je imago weg en kost het minstens een jaar om dit weer op te bouwen.

Merken jullie dan ook dat er minder patiënten komen naar aanleiding van zo'n effect?

Ik denk dat het effect qua aantal patiënten niet zo groot zal zijn, dat is mijn vermoeden, omdat mensen toch een beetje een band hebben met een ziekenhuis. Maar de hele wereld, de hele pers valt over jou heen. Je krijgt ontzettend veel negatieve publiciteit en dat is iets wat je niet wil.

Hebben jullie ook een crisisplan?

We hebben een crisis coördinator, maar dat is niet alleen voor ICT. Maar ook voor grote rampen, zoals een aanrijding op de snelweg met 50 gewonden. We hebben een paar keer een probleem gehad. Dit is niet persé een probleem met de informatiebeveiliging, want dan moet je al snel van die dure externe bureaus inschakelen. Het probleem was de beschikbaarheid van de infrastructuur. Het netwerk lag eruit voor een halve dag, terwijl de poli's moesten draaien. Dit heeft ook met informatiebeveiliging te maken, namelijk de beschikbaarheid van de data. We hebben dit vaker meegemaakt, zowel in het groot als in het klein. Daarom hebben we en continuïteitsplan ontwikkeld. Dat is een heel verhaal van hoe we het hebben ingericht, wat we hebben gedaan om te voorkomen dat dit gebeurt, bijvoorbeeld redundantie. Maar zelfs al heb je redundantie, kan het alsnog fouten gaan. We hebben een keer gehad dat er twee of drie dingen niet goed gingen. Toen ging het netwerk eruit. Dit was echt een enorme toevallig samenloop van omstandigheden. Maar als het kan gebeuren, dan gebeurt het. In dit soort gevallen, hebben we een crisisteam. Dit wordt meestal aangestuurd door iemand in de zorg, want er moeten besluiten worden genomen zoals laten we de poli's doorlopen of niet. Wij moeten steeds een inschatting geven hoe lang het duurt voordat het hersteld is. Je zit daar gewoon met een groep van twintig man, want de hele operatie van het ziekenhuis ligt stil. Het is dan een ziekenhuis breed probleem. Als de infrastructuur niet draait, werken de poli's niet. We hebben wel een back-up systeem daarvoor, maar dat werkt alleen maar voor de kliniek. Dit houdt dat we twintig à dertig laptops hebben waar we dagelijks de belangrijkste databases opzetten, een soort van back-ups. Die brengen we dan naar de klinieken zodat er actuele informatie is over de patiënten. Dit is belangrijk omdat de veiligheid van de patiënt niet in gevaar mag komen.

Testen/trainen jullie ook wel eens op zulke crisis situaties?

Niet zo heel veel. Zulke crises gebeuren met enige regelmaat. Dus feitelijk worden we dan getest. Na afloop van zo'n gebeurtenis doen we een zeer uitgebreide analyse. Aan het einde van de analyse doen we enkele aanbevelingen en die werken we dan af. Dus in principe doen we dit met enige regelmaat. Soms zijn de crises heel groot, als het hele netwerk eruit ligt, heb je niks. Als je data opslag eruit ligt heb je niks. Maar soms is het een applicatie, dan is het een stuk kleiner. Dat wordt dan ook nog op ziekenhuis niveau geëvalueerd. Wat er wel gebeurt is dat er test wordt gedaan of de dieselgeneratoren het nog doen en daarmee wordt ook een deel van de ICT getest. Want je kijkt of alles blijft draaien, als je de stroom er af haalt.

Wat zijn jullie prioriteiten tijdens zo'n beveiligingslek?

De patiëntveiligheid staat altijd bovenaan. Maar privacy komt er wel vlak achter aan. Dus het is lastig. Als je een lek met data hebt, komt de patiëntveiligheid niet persé in het geding. De patiëntveiligheid komt in het geding als de data niet beschikbaar, maar dan is de privacy niet echt een issue. Dus het is zelden of nooit een combinatie van de twee.

Wat gebeurt er na afloop van een incident?

Als er problemen zijn met infrastructuur wordt er met de minuut bijgehouden wat er allemaal gebeurt. Na afloop wordt er een analyse gedaan waaruit aanbevelingen komen voor verbeteringen. Dit doen we ook op ziekenhuis niveau, maar onze analyse is dan het belangrijkst.

We hebben een functionaris gegevensbescherming, dat is degene die potentiele datalekken moet afhandelen. Bij hem wordt alles gemeld. Hij doet een beoordeling over hoe ernstig het is en besluit of we het moeten melden aan de autoriteiten. Vaak blijft het binnen ziekenhuis, omdat het niet zwaar genoeg was om aan de autoriteiten te melden. Maar we hebben het wel een paar keer gedaan. Uiteraard kijken we iedere keer dat zoiets gebeurt na onze procedures en kijken we of we deze moeten aanpassen.

Dus meestal worden dit soort incidente afgehandeld door de functionaris gegevensbescherming, we hebben nog geen incidenten gehad waar bij volledige crisisteam moest worden ingeschakeld.

Ik ga ervan uit dat de kennis niet altijd aanwezig om alle problemen aan te pakken.

Nee, dat is onmogelijk.

Worden er vaak externe partijen ingehuurd?

Wij zijn er ons van bewust dat we niet alles kunnen weten en ook niet alles kunnen bijhouden qua ontwikkelingen in de markt. Dus af en toe komen er mensen binnen om even te kijken van “hoe gaat het hier? Isa alles in orde? Kunnen er dingen verbeterd worden” Die komen dan een dag per maand om te kijken of alles nog goed gaat.

Heeft u nog dingen waar ik naar moet kijken?

Je kunt als ziekenhuis dit niet alleen. Het is heel belangrijk dat er een NVZ is met CISO overleg, het is heel belangrijk dat er een zorg-CERT is. Hier in het ziekenhuis is er een groepje van mensen die vaak bij elkaar komen. Als ziekenhuizen probeer je ook een stukje

uniformiteit, een stukje kennis ontwikkeling gezamenlijk te doen, want het kan niet alleen. Je kunt het niet zonder leveranciers, je moet samenwerken.

Interview 2 Hospital: IT Manager

Zijn jullie actief op zoek naar vulnerabilities in jullie systeem? Hoe doen jullie dat?

We doen dat op verschillende manier. Ik heb eigen mensen. We hebben iemand die is opgeleid tot Certified Ethical Hacker. Dus die probeert ons netwerk te hacken en meldt het als hij zwakke plekken vindt. Dat doen we vaak als we een applicatie kopen van een leverancier. We gaan die dan eerst testen. Hierdoor weten we of we extra maatregelen moeten nemen.

Een ander ding dat we doen is dat we externen in huren om ons te laten hacken. Dat gebeurt ongeveer één keer per jaar. Voor een week of twee, probeert een extern bedrijf ons te hacken. Soms doen ze dit vanaf een afstand, maar soms komen ze ook langs. Dit zijn vaak van die professionele hack bedrijven. Hieruit komen dan lijsten met problemen.

Zijn dat lange lijsten?

In het verleden hebben we echt lijsten van honderden problemen gehad. Maar de urgentie per probleem verschilt. Het probleem bij informatie beveiliging is dat er altijd een probleem is. Maar het is wel het handigste dat je begint met het oplossen van de grootste problemen. Zo werken wij van de grootste problemen naar de minder grote problemen. Maar de werkelijkheid is dat je vaak blijft zitten in het oplossen van de meest kritische problemen en dat het erg moeilijk is om een stapje verder te gaan.

U zei net dat u ook externe applicaties test voordat ze worden toegepast. Schort hier vaak wat aan?

Ja, dat is echt nodig. We hebben wel eens een patiënten portaal gehad. Dat hebben we zelf laten hacken en toen bleek het gewoon lek te zijn. Daarom hebben we dat portaal toen niet in gebruik genomen. Dus het is echt nodig. Soms heb je ook nog een discussie met de leverancier die dan vindt dat het niet lek is. Dat geeft misschien ook de schimmigheid weer, want het is niet zwart-wit. Het is een grijs gebied.

Hebben jullie ook een CVD programma?

Ja, bij ons op de website staat daar een procedure voor. We hebben twee keer gehad dat er meldingen waren gemaakt. Soms zijn dat mensen die gewoon op zoek zijn naar werk. Dat zijn soms bedrijven die willen laten zien hoe goed ze zijn.

Worden die dan ook ingehuurd?

Nee, dat hebben we nog ooit gedaan. Soms zijn het ook script kids. Gewoon jongens van een jaar of 16 die wat scripts en spullen, die zij op het internet gevonden hebben, loslaten op ons netwerk. Daar komen ook zwakheden uit.

Dus zelfs met 'standaard" tools slagen ze erin lekken te vinden?

Ja, dus zelfs met standaard tools kan je nog ergens komen. Maar dat proberen we uiteraard te voorkomen. Want bij elke nieuwe versie van software zijn er weer nieuwe vulnerabilities. Oude applicaties moeten met de nieuwe software kunnen werken en dat gaat niet altijd goed. Dit is er problematisch. Ik zeg wel eens: wij hebben een applicatie die gebruikt van een versie van Staroffice dat gemaakt is voor Windows 95. De leverancier vindt dat die applicatie goed is. We betalen hem nu gewoon niet meer het volledige bedrag. Bijvoorbeeld het kost €20.000 per jaar om dat programma te kunnen gebruiken. Dan zeg ik: 'ik betaal niet meer dan €10.000 per jaar omdat ik vind dat jij dat niet goed doet". Dus aan de ene kant hebben we software uit 1995 en aan de andere kant hebben we de moderne IPhones en IPads. Dat is soms heel ingewikkeld om dat allemaal werkende te maken. Je hebt dan ook nog verschillende lagen in de software zitten. Je hebt infrastructuur, je hebt Windows, maar je hebt ook lagen die daar tussen zitten, bijvoorbeeld Java en database software. Dit zijn voorbeelden van middleware en daar zitten soms bekend lekken in. Het probleem is dan dat de applicaties die gebruikt maakt van die middleware die is getest op die versie van de middleware. Dus ik kan niet zomaar de middleware gaan updaten, want dan doet de applicatie het niet meer. Dus het lijkt heel makkelijk, gewoon alle software updaten. Maar het probleem is, ten eerste moet je het testen en werkt het dus heel vaak niet. Daarnaast moeten die leveranciers het ermee eens zijn, want zij zeggen vaak: "mijn software werkt goed met die versie van Windows en die versie van java". Ook al weten we dat er in die versie, een lek kan zitten, kunnen we niet updaten.

Daar hebben we wat voor, namelijk 'virtual patching'. Normaal noem je dat patching, dat is eigenlijk een plakkertje dat je op een lek plakt. Dan is dat lek afgeschermd. In onze antivirus software zit een module die herkent als andere software een bekend lek probeert te misbruiken. Dus als een lek op een bepaald manier benaderd wordt, ziet de antivirussoftware dat en blokkeert verkeerd gebruik.

Gebeurt het ook vaak dat normale werknemers komen met een mogelijke vulnerability/lek?

Nee, niet met lekken. Maar wel dat iets niet goed werkt. Dat is dan meer functioneel, dat iets het niet doet. Voor hun is dat erg, want ze kunnen dan hun werk minder doen. Vooral als er patiënt voor je neus staat.

Wie behoort er tot het cyber security team? Het team dat zich bezig houdt met cyber security.

We hebben een eigen CERT. Daarin zitten de CISO, een aantal mensen van systeembeheer en ik, als voorzitter van die club. Op het moment dat we bijvoorbeeld zo'n responsible disclosure melding krijgen dan gaan we dat met de CERT hoe we moeten reageren. We behandelen het als een prio 1 melding. We kunnen dan bijvoorbeeld besluiten om een internet verbinding te verbreken, of een applicatie stop te zetten. Maar het kan ook zijn dat het allemaal wel mee valt.

Hoe zorgt u ervoor dat up-to-date blijft over de nieuwste dreigingen?

De software die vandaag nog veilig is, kan morgen onveilig zijn. Dan is er aan de software niet verandert, maar dan heeft iemand iets ontdekt dat niet klopt.

Hoe zorg je ervoor dat je zoveel mogelijk up-to-date bent? Wordt er bijvoorbeeld met een andere externe organisatie samen gewerkt?

Er zijn structuren vanuit de overheid van waaruit wij bepaalde meldingen krijgen, bijvoorbeeld die zorg-CERT, maar ook collega ziekenhuizen. Alle CISO's hebben een eigen netwerk waarin ze communiceren over dreigingen. Dus daar komen ook dingen binnen. Maar ook in het nieuws. Dus als er bijvoorbeeld in het nieuws is dat een bedrijf in Oekraïne besmet is met ransomware, gaan wij wel even kijken. Bijvoorbeeld laatst met Maastricht. Dan gaan wij kijken, wat is daar gebeurt en wat kunnen wij daar mee?

Wat zijn volgens u de grootste dreigingen, het grootste risico?

De grootste dreiging zit bij de gebruiker, via email. Bijvoorbeeld phising, maar ook attachments. Dus Word-bestanden waar bepaalde ransomware of andere virussen zitten. Dat is een heel groot probleem.

Weten jullie ook wat voor andere partijen jullie systemen zouden willen binnendringen?

Nee, dat is wat schimmiger. Het hangt er van af welke motieven er achter zitten. Je kan een financieel motief hebben, bijvoorbeeld bij ransomware. Je hebt natuurlijk ook andere overheden, bijvoorbeeld de Chinezen en de Russen. Bijvoorbeeld, nu met de situatie in Iran

en de Nederlandse militairen die actief zijn in die regio, zijn wij ervan bewust dat wij een mogelijk doelwit zijn. Wij zijn semi-overheid, dus dat kan aantrekkelijk zijn voor het buitenland.

Hoe zorgt u ervoor dat normale werknemers niet op, bijvoorbeeld, verkeerde linkjes drukken?

Aan de ene kant proberen we dat technisch te voorkomen. Je kan een deel afvangen. Wij blokkeren bijvoorbeeld bepaalde soorten bestanden. Dat is wel heel bot. Het is een soort uitgebreide spamfilter. Wij zeggen gewoon als er aan een mailtje een ZIP bestand zit, blokkeren we dat mailtje. Soms betekend dat dat iemand zegt: 'ik krijg mijn mail niet binnen". Het probleem is dat ZIP bestanden ook een soort van zijn versleuteld. Daardoor kan de antivirus software niet goed kan kijken of het bestand veilig. Wat antivirussoftware eigenlijk doet is at het kijkt of ze een bepaalde serie van enen en nullen herkennen als slechte software. Het probleem met encryptie is dat die enen en nullen door elkaar worden gehusseld. Daardoor kan de antivirus dit niet meer herkennen als een virus. Dit gebeurd vaak bij ZIP. Wij hebben een stuk of 20 à 30 bestandstypen geblokkeerd.

Maar ook de antivirus software helpt hier bij. Als opeens bij allemaal verschillende bedrijven hetzelfde mailtje binnenkomt, dan zegt de antivirus dit is spam en dit gaan we blokkeren.

Worden bijvoorbeeld ook mensen getraind om dit tegen te gaan?

Ja, we doen af en toe wat testen. Dan wordt erg gewoon een mailtje gestuurd en gaan we meten, hoe veel mensen erop klikken. Ik kreeg hem zelf ook. Het grappige was, ik kreeg dat mailtje ook, maar ik was gewoon met mijn werk bezig. Ik zag dat dat mailtje van Mijn Overheid was en ik dacht al wat raar dat er een linkje instaat. Ik weet namelijk dat de overheid geen linkjes verstuurd. Ook zat er een attachment aan. Ik heb dus op beide niet geklikt en het mailtje doorgestuurd naar de CISO. Waarna een antwoord kreeg van: "Je bent geslaagd! Dit was onze test". Dit zit soort testen gebeuren dus ook in de zorg. De voorlaatste keer ging over een "fiets voor niets" of je kan een taart winnen ofzo. Maar ik was dus gewoon met mijn werk bezig en ik wist dat er zo'n test zou komen, maar ik had helemaal niet met elkaar gelinkt. Het is ook wel een gebeurt dat we een phishing-mail ontvingen en dat we een melding kregen dat iemand erop geklikt had. Dan ben ik gewoon benieuwd, hoe is dat gegaan. Dan vraag ik "heb jij zo'n mailtje gehad" waarop zij bevestigend antwoorden. En dan vraag ik "wat heb je ermee gedaan". Dan antwoorde die persoon "ja, mijn moeder is net vorige week overleden en ik ben bezig met de financiële afhandeling daarvan. Dus allerlei bedrijven gaan mij mailtjes sturen

over dingen die ik af moet ronden. Ik dacht dat dit daar ook mee te maken had.”. Of mensen die zeggen “morgen ga ik op vakantie, dus ik wilde alle mailtjes die ik had nog even snel afwerken. Dus sorry ja, ik heb even niet goed nagedacht.” Dat is wat er gebeurt, er wordt urgentie gecreëerd en het is even snel klikken en dan is het al gebeurd.

Je probeert het echt te voorkomen door de meeste mailtjes niet door te laten. Dus er blijft een afhankelijkheid van de gebruiker, die moet snappen dat hij niet overal zomaar op moeten klikken.

Is er altijd iemand aanwezig die kan reageren op incidenten? Bijvoorbeeld als gevolg van zo’n phishing mailtje.

Formeel hebben we daar geen afspraken over er is wel 24/7 bereikbaarheid van de ICT. Maar ik weet wel zeker dat de ict mensen aan de gang gaan als ik ze om drie uur ’s nacht bel.

Is een beveiligingslek mogelijk in het ziekenhuis?

Ja

Is het ook wel eens gebeurt?

De term beveiligingslek is natuurlijk heel breed. Het kan zowel groot als klein zijn. Een voorbeeld van een groot lek was zo’n script kid die succesvol was met zo’n standaard stukje software, een SQL injectie in dit geval. Dat houdt in dat je op een invulscherm, waar je normaal je contactgegevens invult, een bepaald programmaatje uitvoert die je toegang geeft tot de achterkant. Ofwel toegang tot de webserver. Als dit niet goed geprogrammeerd is, dan kan het zijn dat de script kiddie’s programmatje gaat uitvoeren. Dus in dat geval was er een script kid, die het lukte om bij zo’n invulscherm zijn programma uit te voeren. Vervolgens kreeg hij een hele database te zien, in dit geval van alle huisartsen in de regio.

Je doet heel erg je best om dit te voorkomen, maar alles is in beweging. Iets wat vandaag veilig is, kan morgen onveilig zijn. Dus dit kan gewoon gebeuren. Wij vragen ons ook niet af ‘of’ het gebeurt, maar ‘wanneer’.

Hoe zorg je ervoor dat er zo snel mogelijk een lek gedetecteerd kan worden?

Dat kan op verschillende manieren. Mensen kunnen het melden, maar we doen ook een stuk monitoring. Dat gaat via een SOC, Security Operating Center. Dat is een externe partij. We hebben op verschillende plekken in ons netwerk “voelers” zitten. Deze “voelers” doen niks anders dan kijken of ze gekke dingen voorbij zien komen. De externe partij houdt dit in de

gaten en dat doen ze 24/7. Het interessante is dat we hierin ook een soort van ontwikkeling doen. Bijvoorbeeld, iemand komt binnen en slaagt erin om een laptop te verbinden met ons netwerk. Deze persoon begint dan ons netwerk te scannen op bekende lekken. Deze scannen kunnen worden gedetecteerd en dan gaan er alarmbellen af bij de SOC. De SOC neemt dan vervolgens contact op met ons. Zo hebben we dus verschillende maatregelen en we zijn continue bezig met de SOC om nieuwe detectiemethodes te ontwikkelen.

In het begin was dat SOC heel erg van we zien een bekend virus, maar nu proberen ze te kijken naar hoe een hacker te werk gaat en dat te herkennen.

Is het dat meer dat ze op zoek zijn naar dingen die anders zijn dan normaal?

Ja inderdaad, ze zijn op zoek naar afwijkend gedrag. Dus bijvoorbeeld een scan van het netwerk is afwijkend gedrag. Normale software gaat niet zomaar een scan maken van ons netwerk. Dat is dus afwijkend gedrag.

Wat gebeurd als er verdacht gedrag wordt gedetecteerd?

Dan wordt dat telefonisch bij ons gemeld, afhankelijk van de urgentie. Dan is het aan ons om hier iets aan te doen.

Is er een crisisplan of iets dergelijks voor een crisis zoals een groot datalek?

In dat geval is er een algemeen crisisplan. Dat kan gebruikt worden als er een groot ongeluk op de snelweg is geweest, waardoor ons ziekenhuis moet opschalen. Dit kunnen ook interne crises zijn, zoals een ICT storing of een iemand die met Ebola het ziekenhuis binnenloopt. Dus er zijn structuren voor alle soorten crises.

Wordt er getraind of getest voor dit soort crises? Bijvoorbeeld een simulatie van een datalek.

Recent is er een hack uitgevoerd en we hadden ook gehoopt dat daar een calamiteit uit zou komen zodat we konden oefenen. Ze gingen helaas net niet ver genoeg, dus dat was niet het geval. Er wordt niet veel geoefend.

De normale calamiteiten worden wel regelmatig geoefend, zoals een stroomstoring of iemand met Ebola.

Stel dat er een datalek is, wat is uw dan een grootste prioriteit?

Dat is afhankelijk van het soort lek. Dan moeten we gaan kijken wat er nodig is om dat lek dicht te zetten. Een voorbeeld zijn de radiologen. Zij hebben thuis een computer staan die direct verbonden is met het ziekenhuis netwerk, zodat ze dag en nacht kunnen kijken naar radiologische beelden. Bijvoorbeeld als iemand binnenkomt met een hersenbloeding, kunnen ze die beelden in detail thuis bekijken. De radiologen zeggen dat dit nodig is, want zonder deze werkwijze kunnen ze geen goede zorg leveren. Als ze naar het ziekenhuis moeten komen, voor het bestuderen van de radiologische beelden, duur dat te lang en kan dat ernstige gevolgen hebben voor de patiënt. Het bleek dat die verbinding versleuteld was op een manier die niet langer veilig was. In dit type versleuteling zat een lek. In eerste instantie, leek het erop dat dit lek niet heel erg was, maar de urgentie nam snel toe. Om 17.00 ’s middags was het duidelijk dat wij iets moesten doen. Toen hebben overleg met de CERT en daar kwam uit dat deze verbinding verbroken moest worden. Ook hebben we toen contact gehad met de raad van bestuur en de radiologen. De radiologen zeiden dat dit echt iets betekend voor onze patiënten. Zij begrepen dat het lek dicht moest, maar legde de nadruk op het feit dat dit niet weken zo kon blijven. Dit betekend gewoon dat iemand schade overhoudt als die nu binnenkomt bij de spoedeisende hulp. Dus dit geeft aan hoe lastig het kan zijn. Gelukkig hadden we de volgende dag het lek gedicht en werkte alles weer

Er is dus eigenlijk een constante balanceer act tussen patiëntveiligheid en dataveiligheid.

Ja klopt, het kan zijn dat ik een verkeerd mailtje stuur. Bijvoorbeeld ik stuur jou een mailtje die ik eigenlijk naar een collega had willen sturen. Dit mailtje wordt verstuurd naar het verkeerde emailadres omdat ik een typefoutje maak en de namen erg op elkaar lijken. In dit mailtje staan patiëntgegevens. Doordat ik nu de patiëntgegevens na de verkeerde persoon heb gestuurd, is er al een datalek. Maar dit datalek heeft niets te maken met continuïteit, omdat alle systemen het nog doen. We moeten dit wel melden. Dus op het moment dat het lek nog bestaat, moet je misschien maatregelen nemen die iets beteken voor de bedrijfsvoering, maar als dat lek niet meer bestaat of niet meer urgent is, dan is het afweging wat je gaat afzetten of uitzetten.

Dat lek bij de radiologen, bestond al een tijdje. Om 17.00 kregen wij te horen, vanuit de zorg-CERT, dat statelijke actoren dit lek misbruikte. Dat kan betekenen dat hetzelfde lek bijvoorbeeld bij Ministerie van Defensie misbruikt werd. Wij worden dan geïnformeerd over dit misbruik en plotseling wordt de urgentie een stuk hoger. Dan moeten wij actie ondernemen. Het is dus lastig.

Elke week zijn er Windows updates. Maar als ik dat altijd doe, moet ik het ziekenhuis uitzetten. We weten gewoon dat er Windows updates en dat deze niet op elke computer in het ziekenhuis geïnstalleerd zijn, maar moet ik dan alle computers uitzetten? We weten dat er lekken zijn en daar hebben we allerlei hekjes om heen staan. Maar je kan van buiten berichten krijgen waaruit blijkt dat jouw maatregelen niet langer voldoende zijn.

Stel dat er een kleiner incident is gebeurd, zoals het sturen van email naar een verkeerd adres, wat gebeurt er dan?

Dat moet je melden, er is een meldplicht. Volgens mij doet de CISO dat. Je kan beter te veel melden dan te weinig. Je ben wettelijk verplicht om dit binnen 72 uur te melden. Daarna kan je verdergaan met je evaluatie.

Als er een groter crisis is geweest, wordt dit ook geëvalueerd? En wordt met de 'lessons learned' ook iets gedaan?

We hebben dus dat CERT overleg en dan kijken we dus wat er gebeurd en wat we kunnen leren.

Heeft de CERT dan ook de leiding tijdens zo'n beveiligingslek?

Nee, uiteindelijk is de raad van bestuur de baas

Maar in de praktijk, wie onderneemt er actie?

Wij ondernemen actie, maar gaan dan met de raad van bestuur overleggen en andere partijen. Als het dan overgaat tot een crisis dan gaan we naar de normale crisisstructuren.

Worden er vaak extern partijen bijgehaald voor bijvoorbeeld crisis situaties?

We hebben nog geen grote crisis gehad en nog geen externe bedrijven moeten inhuren voor een crisis. Maar de eerlijkheid gebied te zeggen dat dit wel ken gebeuren. Die externe partijen bieden zich ook aan. Soms zijn het ook hele grote partijen zoals FOX-IT. Ik heb wel eens gehad, dat wij een storing hadden. Toen werden wij gebeld door iemand van FOX-IT en die gaf aan dat zij ons konden helpen als deze storing het gevolg was van ransomware of een virus. Hiervoor hadden wij nog nooit contact gehad met FOX-IT. Dus dat is gewoon heel commercieel. Die partijen worden ingehuurd, maar dat gaat om waanzinnige bedragen. Die jongens komen niet voor €200 langs.

Zij hebben waarschijnlijk ook heel specialistische kennis die zelden nodig is en komen alleen als het echt serieus is.

Ja klopt. De structuren waar wij nu op zitten is van een crisis kan ontstaan, waarbij we zelf niet precies weten hoe of wat. Maar voor ons is vooral het forensische van belang, dus veel logging en gegevens opslaan. Hierdoor kunnen we achteraf kijken wat er gebeurd is. Dat is het probleem want vaak weten ze niet precies hoe iets gebeurt. Dus door logging en ander methodes hopen wij dit wel te kunnen doen.

Gebruiken jullie ook veel externe producten?

Ja, die SOC, de Firewalls. We maken vaak ook bewust gebruik van meerdere partijen. Bijvoorbeeld op elke computer is een virusscanner geïnstalleerd. Daarnaast hebben we een firewall. Daar gaat al het netwerkverkeer doorheen en scant ook voor virussen. Die firewall is van een ander merk. Dat doe je omdat het kan zijn dat de ene leverancier al na 5 minuten in de gate heeft dat er iets aan de hand is en de andere pas na 3 uur. Je probeert met verschillende leveranciers op verschillende plekken in je netwerk bepaalde risico's zo snel mogelijk te ontdekken. Informatiebeveiliging is ook gebaseerd dat je niet alles op één plek neerzet. Ik vergelijk het altijd met een kasteel. Daar heb je een slotgracht, een valhek, een hoge muur en nog een ridder. Ik ben dan zelf die ridder. Je creëert dus meerdere lagen. Het doel is om bedreigingen aan de buitenkant te stoppen. Maar ook aan de binnenkant moet je beveiliging op orde hebben.

Maar is het dan ook weer zoeken naar een balans waar dokters en verpleegkundige wel hun werk kunnen doen?

Ja, dat is altijd een probleem. De beveiliging staat altijd op gespannen voet met gebruikersgemak. Dat betekend nogal wat. De dokter zegt "ik heb hier een patiënt voor me neus en ik kan niet drie keer in de rondte dansen en dan hoera roepen voor de veiligheid".

Levert dit dan wel eens problemen op?

Het levert wel eens problemen op. Je gaat gewoon verschillende beveiligingsmaatregelen instaleren en het is gewoon zo dat die maatregelen ervoor zorgen dat de normale software niet goed werkt. Outlook doet het wel, maar we hebben hier hele bijzondere software, bijvoorbeeld een EPD. Er zijn drie andere ziekenhuizen die dezelfde software gebruiken. De virusscanner heeft die software ook nog nooit gezien en die ziet daar misschien wel bepaalde

dingen die die dan blokkeert. Dus dat gaat af en toe mis. Dat betekend dus dat iemand zijn werk niet goed kan doen door de veiligheidsmaatregelen.

Interview 3 Hospital, Chief Information Security Officer (CISO)

Hoe wordt er in uw organisatie gezocht naar zwakheden/vulnerabilities?

We hebben een externe partij die scant ons netwerk, maar alleen het server deel. Dat zijn zeg maar 500 van de drieduizend machines ongeveer. Maar dat zijn wel de belangrijkste. Daar krijgen we een rapport en daarmee moeten wij aan de slag. We zijn nu bezig met de meest kritieke bevindingen. Er zijn vier categorieën en we zijn nog in de bovenste categorie aan de slag. Daar zijn behoorlijk wat bevindingen en het is lastige materie. We hebben ook een mechanisme in onze virusscanner die zelf scant en misbruik voorkomt. Aan onze buitenkant wordt ook nog gescand door verschillende leveranciers. We hebben het Z-CERT (zelfde als Zorg-CERT). Dat is een partij die vooral in de zorg actief is.

Is dat een overheidsorgaan?

Het is denk ik een BV die vooral door ministerie ingehuurd wordt. Zij hebben ieder ziekenhuis in Nederland als klant en zijn nu ook bezig met allerlei andere zorginstellingen als klant te krijgen. Zij monitoren onze buitenkant. We hadden bijvoorbeeld net voor de kerst een lek op onze thuiswerkoplossing dan krijgen we een signaaltje van hun, let op je staat op de lijst.

Dit ging vooral over externe partijen, gebeurt dit ook intern?

Intern ook, want als het bijvoorbeeld Microsoft is dan weten we het zelf veel beter, want dan zijn er zo veel lekken en updates. Maar voor andere leverancier is het wat lastiger normaal gesproken.

Is het ook lastiger om al die producten van verschillende leveranciers met elkaar samen te laten werken?

Bijvoorbeeld, ons EPD gebruikt allerlei lagen eronder. Er is een bepaalde database software, we hebben verschillende soorten databases. Op het moment dat er een lek is in een database en je wilt dit gaan patchen dan, moet je wel weten dat je EPD daarna nog werkt. Dat maakt het lastig, want vaak zijn dat bundels, een bepaalde database versie met een bepaalde programma versie samen. Op het moment dat er een lek wordt dat een keer opgelost in een volgende versie van het programma, maar er zit vaak ook een nieuwe functionaliteit die ervoor zorgt dat dingen wel of niet werken. Dus je bent uitgebreid aan het testen.

Dus je bent constant bezig?

Ja en je loopt per definitie achter.

Gebeurt het ook wel eens dat normale werknemers, zoals dokters en verpleegkundigen, naar jullie toe komen omdat iets niet werkt of niet veilig is?

Op veiligheidsgebied zit het hem vooral in “ik krijg een raar mailtje. Andere dingen heb ik niet zo veel voorbeelden van.

Krijgen jullie af en toe wel berichten van werknemers dat iets niet werkt?

Ja dat wel, maar dat is voor de helpdesk. Zij komen niet bij mij. Eventueel stuurt de helpdesk dit door naar mij.

Zijn er ook wel eens close-calls geweest? Dat het bijna goed ging.

Dat is het verhaal van die radiologen. Dat is op zich wel goed gekomen, maar het was wel dat we erg laat waren met patchen door allerlei omstandigheden. Waardoor ze eigenlijk zeiden dat je er wel van uit kon gaan dat je gehackt was als dit lek nog niet gepatcht was. Maar we hebben dat laten onderzoeken en dat bleek bij ons niet het geval te zijn. Dus we zijn de dans ontsprongen.

Dit heeft dan ook te maken, denk ik, met wat je net zei, dat het lastig om altijd up-to-date te blijven.

We hadden wel signalen gekregen, maar niet geïnterpreteerd dat dat bij ons ook draaiden. Je moet je voorstellen dat je echt heel veel meldingen krijgt en dan moet je kijken wat bij jou van toepassing is. In dat proces is iets mis gegaan.

Hoeveel meldingen komen er dan?

Ongeveer 50 à 80 per week.

En zit daar dan ook verschillende urgentie aan?

Ja, maar dat veranderde dus ook nog, want deze was eerst niet zo urgent totdat we actief misbruik zien. Dan wordt het ook een stuk urgenter.

Kunnen jullie dan wel al die meldingen actief gaan onderzoeken? Hebben jullie daar de tijd voor?

Als het echt urgent wordt, dan gaan er vanzelf allerlei andere alarmbellen rammelen. Want daar hebben we contracten mee met leveranciers die ons daarbij helpen. Het zit hem vooral in die dingen die niet zo urgent dat die alarmbellen afgaan, maar wel mis kunnen gaan.

Uit hoeveel mensen bestaat het team dat zich bezig houdt met cyber security?

Ik ben zelf geen leidinggevende. Dus ik moet het doen met de mensen die ICT mij levert. We hebben een CERT en daar zitten twee systeem beheerders, de IT manager en ik in. Dus dat zijn wel de mensen die het meest met beveiliging bezig zijn.

Dus als er iets gebeurt dan gaan jullie actie ondernemen?

Ja, dan zijn wij de aangewezen personen om dat af te handelen

En dat zijn allemaal mensen met een IT achtergrond?

Ja en ook mensen die iets meer van de beveiliging af weten.

Je zei net dat het heel lastig om up-to-date te blijven. Hoe zorg je ervoor dat je zoveel mogelijk up-to-date blijft?

Er zijn tools voor die ons daarbij helpen. Leveranciers leveren ons rapporten bijvoorbeeld. Microsoft en anderen hebben vaak verschillende classificaties van de urgentie van een patch. Die zie je gewoon in die tools terugkomen.

Met die lijst van servers zijn we nog bezig met de meest kritieke patches. Dan neem je vaak de categorieën daar onder ook meer. Als je op zo'n server, een oudere versie van bepaalde software hebt, zitten daar vaak tien verschillende bekende lekken in. Dus die lossen we dan allemaal in één keer op.

Werken jullie ook met ander ziekenhuizen samen? Want jullie zien veel van dezelfde problemen.

Z-CERT faciliteert daar vooral in. Het samenwerken zit hem nu nog vooral op het beleidsniveau. Dus beleidsstukken uitwisselen enzo, niet zozeer deze kennis.

Wat is volgens jou de grootste dreiging/het grootste probleem?

Als je kijkt naar wat wij aan interne risico analyse hebben gedaan, is het vooral de bewustwording van de medewerkers. Die klikken op linkjes waar ze hun wachtwoord achterlaten. Dat hebben we als hoogste risico aangemerkt. Vanuit privacy is het dat mensen kijken in dossiers waar ze niets te zoeken hebben. Ik ben dus nu ook intensief bezig met de

controle van logging beter te maken. Het locken van de werkplek. Als je het ziekenhuis binnenloopt zie je veel open schermen. Mensen lopen weg zonder hun scherm te locken. Dit zijn wel de grootste risico's.

Testen jullie dit ook wel eens?

Ja, in december is er een extern recherche bedrijf binnen geweest en die proberen dan zover mogelijk te komen. Zij zijn bijvoorbeeld ook op OK-sessie geweest. Dat was zeker niet de bedoeling.

Hoe kan je er wel voor zorgen dat de werknemers wel die bewustwording hebben?

Bewustwordingstrajecten. Ik zet met zekere regelmaat een poster op het intranet met en tekst zoals: "de wedhouder is in het ziekenhuis, ik kijk even in zijn dossier, mag dat?". Dat is heel flauw en iedereen weet het antwoord ook wel, maar iedereen is er wel weer even mee bezig. We zijn bezig met externe partijen voor e-learning achtige constructies of met games. Er zijn echt honderden verschillende manieren om mensen ermee bezig te laten zijn.

Wat je ook merkt is dat mensen die in de zorg werken dat met een reden doen. Het zijn vaak mensen die klaar staan voor een ander. Op het moment dat jij binnenkomt op een OK, houden zij de deur nog voor je open, terwijl je er misschien wel niets te zoeken hebt. Ze zijn niet zo argwanend over het algemeen. Ze zouden argwanend moeten zijn, maar dat is niet altijd zo.

Worden ze dan ook wel regelmatig getest? Bijvoorbeeld door het sturen van phishing emails?

Ja, en daar tuinen ze dan met open ogen ook weer in.

Gebeurt dat veel?

Ja, dat is echt schrikbarend. De laatste test die ik gedaan heb, was ziekenhuis breed en was vorig jaar nog. 30% liet zijn gebruikersnaam en wachtwoord achter.

Wat gebeurt er dan?

Er wordt een rapportje gestuurd. Op het moment dat ze klikken krijgen ze een melding op hun scherm waarin staat dat dit niet de bedoeling is en met uitleg over hoe ze dit kunnen herkennen. Maar het verandert niet echt.

Dus het zal altijd een probleem blijven?

Ja, waar wij als IT heel hard aan werken, is om die scan van foute mails heel goed te maken, een soort van spamfilter. Maar ook sites die je bezoekt worden gefilterd. Zo probeer je met allerlei maatregelen, het technisch op te lossen. Maar dat is wel beperkt. Als ze maar goed genoeg een mailtje maken, ziet die spamfilter het ook niet. Dus vroeg of laat gaat het wel een keertje mis. Dat zie je ook bij andere ziekenhuizen regelmatig.

Dit gaat dan ook vaker mis?

Ja, regelmatig. Vorig jaar is zoiets wel gebeurd bij meer dan vijf ziekenhuizen.

Wat moet een werknemer doen als hij er achter komt dat hij net op een verkeerd linkje heeft gedrukt?

Helpdesk bellen.

Daar is dan ook altijd iemand beschikbaar?

Ja, 24/7.

Daar zit dan ook altijd iemand?

Er zit niet altijd iemand. Tijdens kantoortijden zit er altijd iemand en daarbuiten heeft een systeembeheerder altijd dienst en is bereikbaar.

Is een beveiliginslek mogelijk?

Ja

Is het waarschijnlijk dat dat gebeurt?

Als je gaat kijken dat 5 van de 80 ziekenhuizen slachtoffer is geworden van een succesvolle phishing aanval, dan gaat het bij ons vroeg of laat ook een keer gebeuren.

Zijn jullie daarop voorbereid? Hebben jullie daar een plan voor?

Ja en daar hebben we ook al een keer droog op geoefend. We hebben ook al wel ervaring. In 2016 was er een specialist die gebruikersnaam en wachtwoord achter had gelaten en waarbij de mailbox was leeggemaakt door een Nigeriaanse partij. Dat was nog net dat er geen meldplicht voor datalekken was, want ander hadden we wel in de krant gestaan. Maar ja dat zijn wel dingen die gewoon gebeuren. Nu proberen we dat te voorkomen door tweevoudige verificatie toe te passen. Dus dat voor het inloggen op een mail zowel een wachtwoord als een sms-code nodig is.

Hoe zorg je ervoor dat je zo snel mogelijk zo'n datalek detecteert?

We hebben een dienst met een extern partij die kijkt op ons netwerk actief mee. Als zij verdachte dingen zien, trekken zij aan de bel.

Trainen of testen jullie ook regelmatig op dat soort situaties?

Dat is wel lastig hoor, een soort van droogzwemmen. Als je iemand in de diepe zee gooit, kan je ook niet opeens zwemmen. Het beste leer je van echte crises.

Wie zou in zo'n crisis de leiding nemen?

Hangt ervan af hoe ver het is. Op het moment dat er een datalek is, gaan we gewoon FOX bellen.

Ja dat is wel de grote naam, beter wordt het niet

Nee, beter wordt het niet. En ze zijn er ook gewoon voor beschikbaar. Ze adverteren mee en ze hebben de kennis in huis. Als zij er niet uitkomen dan komt niemand eruit.

Er is natuurlijk ook een raad van bestuur. Ik ga ervan uit dat die vaak geen technische achtergrond hebben. Wie neemt er in zo'n geval de besluiten?

Dat valt nog mee, want wij hebben een registeraccountant en die is echt van de details. Die heb ik bijvoorbeeld voor een de invoering van een NEN7510 het hele plan en bijlages opgestuurd. Hij ging gewoon op detail niveau vragen stellen, waarvan ik dacht hoe zit dat ook al weer. Hij is dus wel in staat om daarin de goede beslissingen te nemen en hij gaat ook niet tegen FOX zijn, als wij geraakt zijn. Maar dus dat droogzwemmen oefenen we dus niet met hem, omdat zijn tijd daar tekort voor is.

Wat is de belangrijkste prioriteit in het geval van een datalek of andere crisis?

De zorg gaat altijd voor.

Ook in gevallen van ernstige privacy schendingen?

Ja, dan gaat nog steeds de zorg voor. Als je kijkt naar het Haga ziekenhuis met Barbie. Zij hebben een boete van de autoriteit gekregen. Dat ging dan over controle over de logging, maar ook hoe meld je je aan op de werkplek. Dat moest ook met twee factoren. Dus een personeelspas en een wachtwoord. Bij ons wordt ook gezegd: "dat loopt de zorg te veel in de weg". Dus dat doen we alleen als dat echt wordt opgedragen door de autoriteit. Zo zie je dat beveiliging altijd een afweging is tussen waar is het nog werkbaar en waar is het helemaal

dicht getimmerd. In een ziekenhuis ligt dat echt wat anders dan in een kerncentrale, want daar zijn de gevolgen veel minder als het mis gaat.

Je zei net ook dat één van je taken is cyber security, wat zijn dan je andere taken?

Informatie beveiligingsbeleid. Daar zijn een aantal stukken die je voor elkaar moet hebben om gecertificeerd te raken. Daar beschrijf je in van hoe die structuur in elkaar zit. Het zijn voor de rest veel overlegjes. Ik ben een soort van vraagbaak op het gebied van informatieveiligheid. Als er iets nieuws wordt aangeschaft, kijk ik mee of het veilig is.

Is dat nodig dan om nieuwe producten te checken voor veiligheid?

Ja, we hadden cameraatjes bij onze baby'tjes in het ziekenhuis. Daardoor konden ouders meekijken. Dat was fantastisch allemaal, maar dat was zo lek als een mandje. Het was alleen gebruikersnaam en wachtwoord en dan kon je gelijk alle camera's zien. Dus nu hebben we dat uitgezet en zijn we op zoek naar een beter product. Zo zijn er allerlei dingetjes.

Ik heb ook gehoord dat de ziekenhuizen zelf wel goed in elkaar zitten, maar een probleem zijn de medische apparaten.

Ja klopt, dat is een groot probleem. Het voornaamste probleem is dat deze aangeschaft worden in een gecertificeerde toestand. Dus je koopt een apparaat, die is gecertificeerd, en je mag er niets meer aan veranderen. Op IT gebied, betekend dat er altijd meer kwetsbaarheden bekend worden, maar je mag er niets aan doen.

Is het dan dat zo'n apparaat gecertificeerd is voor medisch gebruik en als je er iets aan veranderd, het niet langer gecertificeerd is?

Ja klopt, zodra er een patch wordt geïnstalleerd vervalt het certificaat.

Betekend dat dan het niet meer gebruikt mag worden voor medische doeleinden?

Ik weet dat niet exact, maar volgens mij is het dan dat het niet meer gebruikt mag worden voor medische doeleinden. Maar het is niet mijn vak dus dat zou je aan iemand anders moeten vragen.

In hoeverre kan jij je werk doen zonder externe partijen?

Niet zonder. Bijvoorbeeld dat 24/7 mijn netwerk in de gaten houden, dat lukt mij niet. Dat is zulke specifieke kennis. Die mensen krijgen is, ook voor hun, een hele grote uitdaging. Dat

gaat ons in ieder geval niet lukken. Er zijn er ook niet zo veel SOC's in Nederland, maar je moet van behoorlijke grote zijn, wil je dat kunnen regelen.

Zij hebben dan ook maar een beperkte capaciteit?

Ja, er zijn gewoon niet zo veel mensen op de markt en je hebt gewoon 10 mensen nodig ofzo, wil je 24/7 goede dekking hebben.

Als we dat alleen voor ons zelf zouden doen dan heb je tijdens kantoortijden er wel eentje, maar daar buiten is er nog veel meer tijd.

Lukt het jullie dan wel om voldoende gekwalificeerde mensen binnen te halen?

Tot nu toe nog wel, maar dat wordt wel steeds lastiger.

Is er dan een groot tekort aan security specialisten?

Bij alles met IT is er een tekort, maar met security nog meer.