

Louvain School of Management

Economic impact of ransomware attacks on the Belgian healthcare sector

How can risk mitigation strategies minimize financial losses and enhance cybersecurity resilience?

Author(s): Romain FERRANT
Supervisor(s): Pr. Bernard Paque
Academic year 2024-2025
Dissertation for the master of Business Engineering specializing in
Financial Engineering
Daytime schedule

Abstract :

Ransomware attacks have emerged as one of the most significant threats to critical infrastructure, with the healthcare sector being particularly vulnerable. This thesis investigates the economic impact of ransomware on Belgian healthcare institutions, combining qualitative and quantitative methods to provide a comprehensive analysis. Through an extensive review of existing literature, insights from interviews with healthcare IT professionals, and case studies of ransomware incidents, the study highlights the financial, operational, and reputational repercussions of such attacks.

The quantitative analysis relies on publicly available data, which is limited due to the lack of detailed information on the financial consequences of ransomware attacks in Belgium. While this constraint limits the scope of the analysis, the study makes the most of the available data to provide valuable insights within the context of a master's thesis. It illustrates the significant direct costs, such as system restoration and ransom payments, as well as indirect costs, including operational disruptions and loss of public trust.

The study concludes with actionable recommendations for policymakers, healthcare administrators, and IT professionals, emphasizing the importance of a proactive approach to cybersecurity. By aligning resources with strategic priorities and fostering collaboration, Belgian healthcare institutions can enhance their resilience against ransomware, safeguarding patient care and public trust.

UNIVERSITÉ CATHOLIQUE DE LOUVAIN
Louvain School of Management

Place des Doyens, 1 bte L2.01.01, 1348 Louvain-la-Neuve
Boulevard Emile Devreux 6, 6000 Charleroi, Belgique
Chaussée de Binche 151, 7000 Mons, Belgique
www.uclouvain.be/lsm

AI Declaration

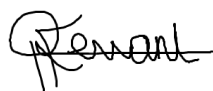
During the preparation of this master's thesis, the author utilized Chat GPT (Version 4o) for the following purpose:

1. **Literature review help:** Chat GPT was used to assist in suggesting relevant pieces of scientific literature and sources that could be used as a baseline for the research and provide additional context.
2. **Summarizing and clarifying:** The AI tool also helped in summarizing large amounts of information, and was employed to refine and express the author's ideas more clearly and professionally throughout the thesis to ensure coherence and precision.

After using Chat GPT , the author diligently reviewed and edited the content produced by the tool. He takes full responsibility for the final content presented in this thesis.

By signing this declaration, he affirms that the content of this master's thesis reflects his original work, augmented by the responsible use of AI.

Romain Ferrant

A handwritten signature in black ink, appearing to read 'Romain Ferrant', with a stylized, cursive script.

Signed the 5th of January, 2025

Acknowledgements

This thesis was the result of several months of intensive reading through scientific literature and press articles, analysis, and thorough writing. This would not have been possible without the support and help of several people.

*First and foremost, I would like to express my deepest gratitude to **my parents**, whose unwavering support and encouragement have been my greatest source of strength. During moments when I lacked the energy or courage to move forward, their motivation kept me going. I especially want to thank my father for dedicating so much of his time to reviewing my text, making insightful additions, and ensuring coherence from an outside perspective. His contributions provided invaluable guidance and support throughout this process.*

*I also want to extend my heartfelt thanks towards **my thesis supervisor, professor Bernard Paque**, for his excellent guidance during the realization of this thesis. His expertise, insightful feedback and precious advice allowed me to steadily navigate through the sea of available information and write a coherent thesis.*

Lastly, I would like to give special thanks to Pierre Colin, CIO of the Saint-Luc hospital in Brussels, to have given me some of his precious time for an invaluable interview.

Contents

1	Introduction: Research context and objectives	1
1.1	Background on ransomware and its relevance to the healthcare sector . . .	2
1.2	Importance of cybersecurity in the Belgian healthcare sector	3
1.3	Overview of the research question	6
2	Methodology	7
3	Literature Review	8
3.1	Defining ransomware	8
3.2	Impact of ransomware on the healthcare sector	9
3.3	Economic magnitude of ransomware attacks on the healthcare sector . . .	12
3.4	Proactive risk mitigation strategies	16
3.5	Reactive vs proactive cybersecurity	16
3.6	Conclusion	19
4	Analysis of the impact a ransomware attack on a Belgian hospital	20
4.1	Analysis of the economic impact of ransomware attacks on the Belgian healthcare sector	20
4.2	Quantitative data on financial losses, recovery costs, and indirect costs . .	21
4.3	Qualitative impact of ransomware attacks	23
5	Proactive Risk Mitigation Strategies	25
5.1	Identification and evaluation of proactive risk mitigation strategies cur- rently in use in the Belgian healthcare sector	25
5.2	Analysis of the effectiveness of these strategies in minimizing financial losses	27
5.3	Case studies or examples of successful implementation of mitigation strategies	28
6	Weighing Cyber Insurance vs. Improved Cybersecurity Practices	29
6.1	Costs and Risks of Cyber Insurance	29
7	Discussion	31
7.1	Interpretation of findings in the context of existing literature	31
7.2	Comparison with other sectors or countries if relevant	31
7.3	Implications for policymakers, healthcare administrators, and IT managers	32
8	Conclusion and Recommendations	35
8.1	Recommendations for improving cybersecurity resilience in the Belgian healthcare sector	36
8.2	Limitations and future research	37

References	38
A Appendices	45

List of Tables

1	Summary of recent cyberattacks on Belgian healthcare institutions	5
2	Estimated costs associated with ransomware attacks on healthcare organi- zations	15
3	Comparison of reactive and proactive cybersecurity approaches	18
4	Summary of financial and operational impacts of ransomware attacks on Belgian healthcare institutions	21
5	Analysis of the estimated cost of the ransomware attack on the CHRSM .	23
6	Effectiveness of proactive risk mitigation strategies in minimizing financial losses	27

List of Figures

1	Distribution of detected cyberattacks worldwide in 2023, by type (Source: Statista)	1
2	Breakdown of cybersecurity threats in the European health sector (Jan 2021-March 2023). (ENISA, 2023)	2
3	Yearly number of cyber-incidents on the European health sector from Jan. 2021 to March 2023. (ENISA, 2023)	3
4	Cost difference from USD 4.88M breach average (IBM, 2024)	45
5	Cost of a data breach by industry, measured in USD millions (IBM, 2024) .	46
6	Cause of the databreach between 3 categories (IBM, 2024)	46
7	Causes of reported ransomware attacks in 2020. (Statista, 2020)	47
8	Number of worldwide cyberattacks aimed at critical infrastructure	47

1 Introduction: Research context and objectives

In recent years, cyberattacks have become one of the most significant challenges for organizations worldwide, with ransomware attacks emerging as particularly prominent and disruptive, as seen in figure 1. These attacks encrypt critical data and demand payment for its release, often crippling operations and causing severe financial and reputational damage. The healthcare sector has become a prime target for such attacks due to its reliance on sensitive data, outdated systems, and the urgent nature of its services.

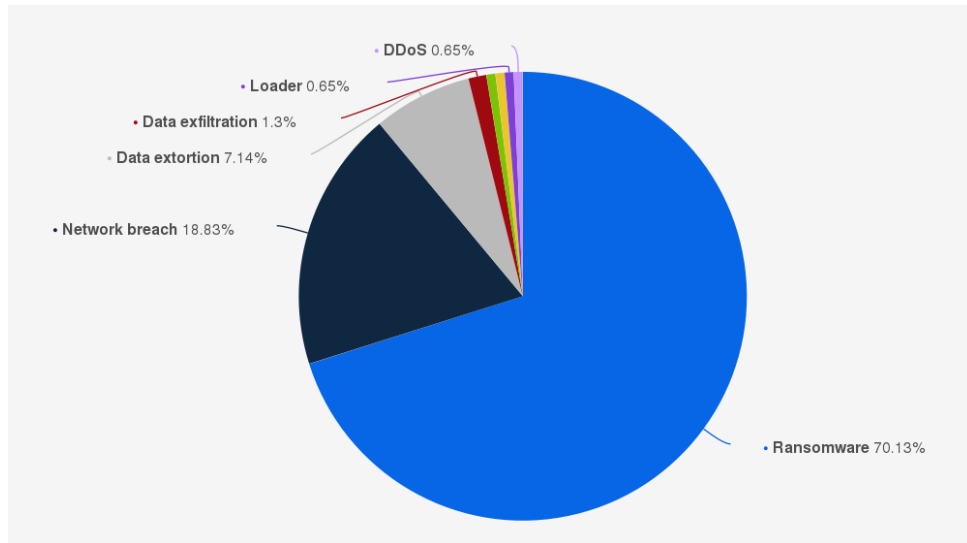


Figure 1: Distribution of detected cyberattacks worldwide in 2023, by type (Source: Statista)

Belgium's healthcare sector is no exception. Designated as critical infrastructure¹ by the National Crisis Center, it plays a vital role in maintaining public health and safety. Any disruption to healthcare services not only affects patient care but could also lead to cascading effects on society and the economy.

This thesis aims to examine the economic impact of ransomware attacks on Belgian healthcare institutions and evaluate strategies to mitigate these risks.

¹« infrastructure critique » : installation, système ou partie de celui-ci, d'intérêt fédéral, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'interruption du fonctionnement ou la destruction aurait une incidence significative du fait de la défaillance de ces fonctions. (crisiscentrum.be)

1.1 Background on ransomware and its relevance to the health-care sector

Ransomware attacks have evolved in sophistication, shifting from opportunistic attacks to highly targeted campaigns against critical infrastructure. The WannaCry ransomware attack of 2017 serves as a landmark example, disrupting healthcare systems globally, including the UK’s National Health Service (NHS). This attack resulted in £92 million in losses to the UK due to operational downtime and recovery costs, with over 19,000 appointments canceled. Globally, it is estimated that this attack caused around \$4 billion in losses (Kaspersky, 2024). Such incidents highlight the critical risks posed by ransomware in healthcare, where the disruption of IT systems directly jeopardizes patient care. Patient data, including medical records, personal identifiers, and financial information, is highly valuable on black markets. Furthermore, the healthcare sector’s reliance on legacy systems and the growing adoption of connected medical devices expand the attack surface, compounding cybersecurity risks.

Illustratively, Figure 2 shows that ransomware accounts for a majority of cyber incidents in the healthcare sector in Europe, demonstrating its dominance as a critical threat for hospitals and health institutions. An incident can be categorised into more than one threat category, meaning that the total percentage of the threats shown exceeds 100%.

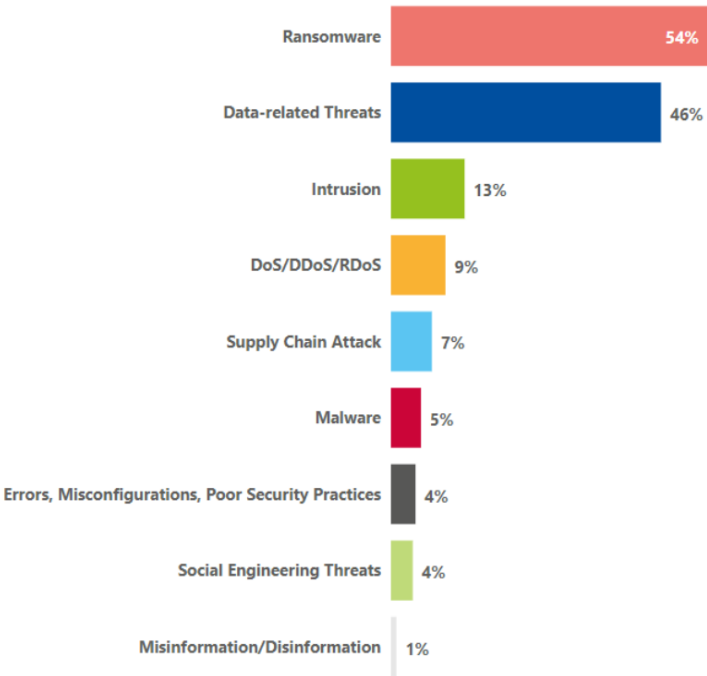
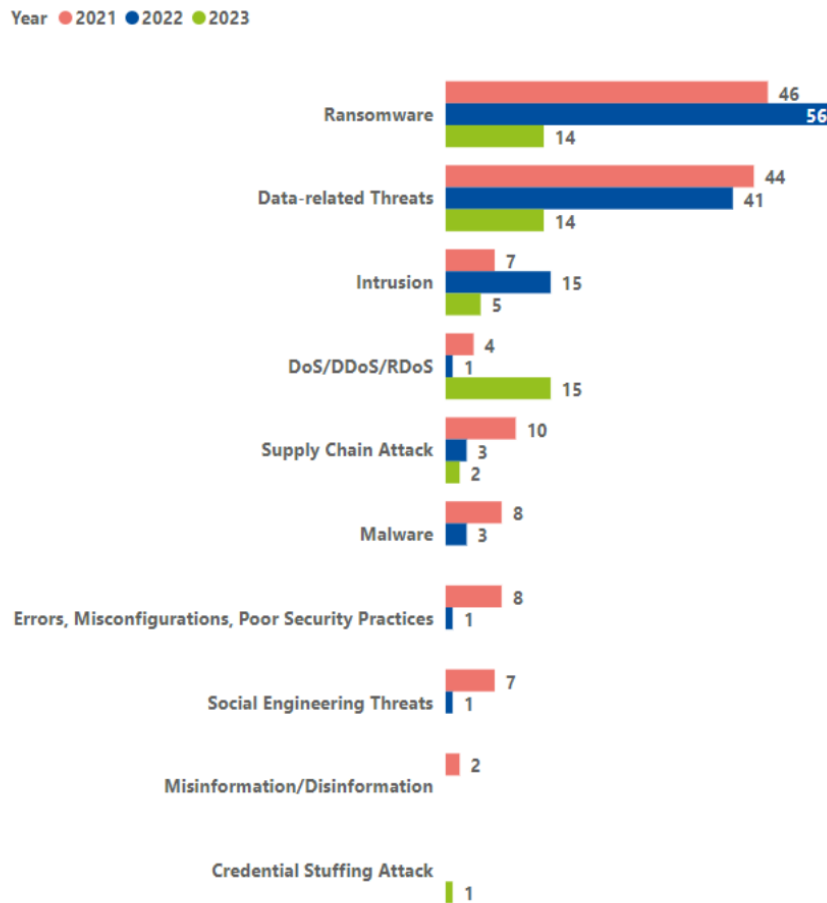


Figure 2: Breakdown of cybersecurity threats in the European health sector (Jan 2021-March 2023). (ENISA, 2023)

1.2 Importance of cybersecurity in the Belgian healthcare sector

As mentioned in the introduction, in Belgium, the healthcare sector is considered a critical infrastructure, highlighting the vital importance of the sector in safeguarding public health and safety. A ransomware attack disrupting healthcare services could trigger widespread consequences, impacting not only our country but also neighboring ones.

Figure 3: Yearly number of cyber-incidents on the European health sector from Jan. 2021 to March 2023. (ENISA, 2023)



Note: An incident can be categorised into more than one threat category. Therefore, the total number of incidents per threat in this figure is greater than the sample of the study (215 publicly reported incidents).

This bar graph provides a historical perspective on the increasing frequency of cyberattacks targeting healthcare in Europe over the last couple of years, emphasizing the importance of addressing this issue. The data used in the research recorded attacks from 2021 up to March of 2023, explaining the much lower number of cyberattacks in that year.

Belgian healthcare institutions have increasingly embraced digital transformation over the last decade, leveraging electronic health records (EHRs), picture archiving and communication systems (PACS), telemedicine, and connected medical devices to enhance patient care (like electrocardiograms (ECG), monitoring devices, etc.). However, this reliance on

digital systems also creates vulnerabilities.

Axel Legay, a professor of cybersecurity at UCLouvain, highlights this growing vulnerability: *“It must be recognized that public structures such as hospitals constitute a prime target for hackers. Especially in recent years, where hospitals are becoming increasingly digital. We ask them to digitize more and more quickly and this often leads to certain shortcomings or oversights in terms of protection.”*

This rapid digitization often leaves gaps in cybersecurity policies, procedures, and systems, which malicious actors exploit (Noulet, 2024).

To illustrate the gravity of the situation, Belgian hospitals have suffered numerous cyberattacks in recent years, ranging from ransomware incidents to unauthorized access to sensitive data. These attacks have affected not only the financial stability of healthcare institutions but also their ability to deliver uninterrupted medical services. The following table summarizes major reported cyberattacks on Belgian healthcare facilities:

Sources:

- Centre Hospitalier Wallonie-Picarde (CHwapi) : (Montero, Mergen, & Wuidart, 2021; RTBF, 2021a; Belga, 2021)
- Clinique de Saint-Luc Bouge: (Clinique Saint-Luc Bouge, 2022; RTBF, 2021b; Dourfils, 2021)
- Ziekenfonds OZ: (Digitale Toekomst, 2021; Heymans, 2021)
- Sint-Andriesziekenhuis: (Verdonck, 2022; Sint-Andries Ziekenhuis, 2022)
- Algemeen Ziekenhuis (AZ) Herentals: (AZ Herentals, 2022; Belga, 2022a)
- Centre Hospitalier Universitaire (CHU) Liege: (Belga, 2022b; Poncelet, 2022)
- Vivalia: (Sente, 2022; Louvigny, 2022; Numerikare, 2022)
- CHC Liège: (Giot, 2022, 2023)
- VZW Curando: (Curando, 2023a, 2023b)
- CHU Saint-Pierre: (RTL info, 2023; Durieux, 2023)
- CHR Sambre et Meuse: (Hennuy & Van Oppens, 2024; Fobe, 2023; CHRSM, 2023)

Table 1: Summary of recent cyberattacks on Belgian healthcare institutions

Date	Institution	Institution Type and Size	Type of Attack	Impact	Financial Implications
18/01/2021	CHwapi, Tournai	General Hospital, 600+ beds	Ransomware	80 servers disabled, emergency services redirected, delayed operations	Estimated recovery costs and operational disruptions: €1M+
09/10/2021	Clinique Saint-Luc de Bouge	General Hospital, 302 beds	Ransomware	Entire IT infrastructure encrypted; approximately 1,000 consultations canceled; critical services disrupted	Ransom of €150 000 demanded; actual financial losses not disclosed
11/09/2021	Ziekenfonds OZ	Health Insurance Fund, National Coverage	Hacking	Unauthorized access, data breach impacting healthcare insurance records	Not disclosed
26/01/2022	Sint-Andriesziekenhuis, Tielst	General Hospital, 270 beds	Malware Attack	Malware detected on one server; swiftly mitigated. No confidential data exposed, and hospital operations continued	Minimal costs due to quick mitigation
20/04/2022	AZ Herentals	General Hospital, 243 beds	Data Breach	Unauthorized access to internal documents. Patient records were not compromised. Steps taken to mitigate the breach included external expert support and notification of authorities	Not disclosed
25/05/2022	CHU Liège	University Hospital, 1,038 beds	Attempted Cyber-attack	Large-scale and prolonged attack successfully defended. Systems remained operational	Not disclosed
14/05/2022	Vivalia Hospital Group	Hospital Group, 1,500+ beds	Ransomware	Disrupted all services, partial recovery after 7 weeks	Estimated costs: €3M+ (operational and recovery)
18/11/2022	CHC Liège (MontLégia)	General Hospital, 840 beds	Attempted Cyber-attack	IT systems disrupted, operations in "red phase". Appointment scheduling limited to phone. Emergency measures ensured critical care	Not disclosed
22/01/2023	VZW Curando Care Facility	Nursing Care Facility, Multiple Locations	Cyberattack	Minimal impact, rapid recovery	Minimal costs due to rapid recovery
11/03/2023	CHU Saint-Pierre, Brussels	University Hospital, 525 beds	Cyberattack	Abnormal activity detected, systems halted briefly	Not disclosed
26/05/2023	CHR Sambre et Meuse (CHRSM)	Regional Hospital, 700 beds	Ransomware	127 GB data stolen, critical services severely disrupted	Estimated costs: €3-5M (data recovery and operational loss)

1.3 Overview of the research question

Despite growing awareness of the threat posed by ransomware, there remains a significant knowledge gap regarding its economic impact on the Belgian healthcare sector. Existing studies primarily focus on technical defenses or global case studies, leaving a need for localized research that addresses Belgium's unique healthcare environment.

This master's thesis seeks to bridge this gap by exploring the following research question:

What is the economic impact of ransomware attacks on the Belgian healthcare sector, and how can proactive risk mitigation strategies minimize financial losses and enhance overall cybersecurity resilience?

To answer the question, the research will adopt a mixed-methods approach, combining quantitative analysis of financial data with qualitative insights from interviews and case studies. This dual approach will provide a comprehensive understanding of the direct and indirect costs of ransomware attacks and assess the effectiveness of various risk mitigation strategies.

2 Methodology

This section serves to outline the methodology that will be employed to analyze the economic impact of ransomware attacks on the Belgian healthcare sector on one hand, and to evaluate the effectiveness of proactive risk mitigation strategies in minimizing financial losses and enhancing cybersecurity resilience on the other. The methodology encompasses data collection, data analysis, and the use of various case studies to ensure an extensive coverage of the subject.

This thesis adopts a mixed-methods approach to explore the economic impact of ransomware attacks on Belgian healthcare institutions and to evaluate the effectiveness of proactive risk mitigation strategies.

First an extensive review of the literature will be presented, focusing on the nature of ransomware, its specific impact on the healthcare sector, the inherent vulnerabilities of healthcare institutions, and an overview of the effectiveness of current mitigation strategies.

The second part of this thesis will present a quantitative and qualitative analysis of the impact of a ransomware attack on a Belgian healthcare institution, incorporating a recent attack as a case study. This case study serves as an analysis of the financial, operational, and reputational consequences of an extensive ransomware attack, providing a real-world example to contextualize the findings. Following this, a practical overview of proactive mitigation strategies will be presented, showcasing their efficiency in reducing financial losses and improving resilience.

The thesis concludes with a set of actionable recommendations based on the findings from the literature review, interviews, and analysis. These recommendations aim to enhance the resilience of Belgian healthcare institutions against ransomware attacks and provide insights for policymakers, healthcare administrators, and IT professionals. Finally, the limitations of this master's thesis as well as suggestions for future research will be presented.

3 Literature Review

The objective of this part is to delve into the literature to obtain a better understanding of ransomware attacks, their impact on the healthcare sector, and the effectiveness of proactive risk mitigation strategies.

3.1 Defining ransomware

Ransomware is a type of malicious software designed to block access to a computer system or data until a ransom is paid. This form of cyberattack has evolved over the years, becoming more sophisticated and damaging. According to the ENISA threat landscape for ransomware, these attacks have adapted to new business models, leveraging the cyber-crime ecosystem for more efficient distribution and execution of attacks (European Union Agency For Cybersecurity, 2022).

One of the most prominent developments is the rise of **Ransomware as a Service (RaaS)**, a business model where ransomware developers lease their software to affiliates who execute the attacks. This has drastically lowered the barrier to entry for cyber-criminals, making it possible even for non-technical actors to carry out sophisticated ransomware campaigns, which has fueled the exponential growth of ransomware incidents worldwide (Coveware, 2022).

The different types of ransomware can be categorized based on the actions it performs and the assets it targets. The ENISA report outlines a classification using the LEDS matrix (Lock, Encrypt, Delete, Steal) (European Union Agency For Cybersecurity, 2022):

- Lock: Ransomware that locks the user out of their system
- Encrypt: Ransomware that encrypts files, making them inaccessible
- Delete: Ransomware that deletes files
- Steal: Ransomware that exfiltrates data for further exploitation

Muslim et al. (2019) further elaborates on these types, highlighting that modern ransomware often combines multiple actions, making it more versatile and harder to combat. A study by Kirubavathi et al. (2024) reviewing recent ransomware attacks on healthcare industries reveals ransomware trends such as "double extortion" (encryption and public data leaks), which highlights the increasing sophistication of attackers.

Once the data has been compromised, the perpetrators demand payment of a fee (a ransom) in exchange for restoring access. Payments are typically requested in cryptocurrencies (for example, Bitcoin), which are more difficult for criminal justice authorities to trace (World Health Organization, 2024).

3.2 Impact of ransomware on the healthcare sector

The healthcare sector in general has relatively recently undergone rapid digital transformation aimed at improving patient care and operational efficiency over the course of the last decade. However, this transformation is often occurring without adequate attention being paid to the new cybersecurity risks it introduces. Healthcare entities, including hospitals, health research- and insurance companies, store large amounts of critical digital information by interconnecting thousands of systems such as patient monitoring systems, electronic health records, and medical imaging acquisition devices. This data, combined with often inadequate security measures and a lack of staff awareness, makes the healthcare sector a prime target for cybercriminals. They exploit these vulnerabilities, aware of the sector's dependence on rapid access to data, particularly during emergencies or crisis situations such as the COVID-19 pandemic, to demand ransoms to unlock critical systems (World Health Organization, 2024).

As Kruse et al. (2017) summarizes, the healthcare sector is falling behind other prominent industries in protecting essential data. Going forward, it will need to constantly adjust to the evolving cybersecurity patterns and dangers, like ransomware, which exploit critical infrastructure and steal important patient information.

In recent years, especially during the Covid-19 outbreak (Chigada & Madzinga, 2021), the European health sector faced a significant number of these cyber-incidents. A study by the European Union Agency for Cybersecurity analyzed 215 publicly reported incidents on the healthcare sector in the EU between January 2021 and March 2023. Healthcare providers accounted for 53% of the total incidents, with hospitals being particularly affected (42%). Incidents targeting health authorities, bodies, and agencies made up 14%, and the pharmaceutical industry accounted for 9% (European Union Agency for Cybersecurity, 2023). Ransomware attacks were responsible for more than half (54%) of these cyber incidents.

To go further, the study analyses the impact from the perspective of the consequences. The cyberattacks frequently resulted in **data breaches** or theft, with 43% of ransomware incidents in the healthcare sector leading to data breaches (European Union Agency for Cybersecurity, 2023).

Over the analysed period, the primary aim of these attacks are mainly patient data and electronic health records, which are targeted in 30% of the cases. This is because patient data are highly valuable, as they are often used for identity theft, fraud, extortion, and blackmail. Patient records not only include personal data but also sensitive health information, thus making them highly valuable on the dark web.

On top of that, the ENISA report shows that ransomware attacks in the healthcare sector often lead to disruptions in healthcare services (cancellation of operations, slower admission of patients, forced rerouting of patients to other hospitals, et cetera.), with 22% of the attacks leading to these consequences. (European Union Agency for Cybersecurity, 2023).

The WHO indeed highlights that through these attacks, patient safety and care delivery can be directly impacted. For instance, if a healthcare organization experiences a cyber-attack, hackers might gain entry to sensitive patient data, such as personal information, medical history, and financial details. In severe instances, cyber-attacks have resulted in the closure of entire healthcare facilities, endangering the lives of patients. Ransomware attacks that block access to crucial healthcare IT systems frequently cause disruptions, leading to the cancellation of outpatient appointments and elective surgical procedures. In more severe attacks, emergency rooms have been forced to divert ambulances, or cancer centers have had to delay treatment for their patients. In the most recent cases, cybercriminals have focused on mental health records, leading to the public exposure of private files. This shows how far the effects of these cyberattacks reach (World Health Organization, 2024).

Vulnerabilities of healthcare systems

The trend is thus that healthcare systems are increasingly targeted by cybercriminals due to their reliance on digital technologies, the high value of their data, and inherent vulnerabilities. This chapter aims to distinguish these vulnerabilities, drawing on insights from recent studies.

The healthcare sector has undergone significant digital transformation, enhancing patient care through electronic health records (EHRs), picture archiving and communication systems (PACS), interconnected medical devices, patient monitoring devices and telehealth services. However, this shift has also introduced substantial cybersecurity risks. Healthcare systems are often considered "soft targets" because they house large amounts of sensitive data and operate on legacy systems that are difficult to secure (Martin, Martin, Hankin, Darzi, & Kinross, 2017). Furthermore, healthcare organizations typically invest less in IT security compared to other industries, making them more susceptible to cyberattacks (Kruse et al., 2017).

There are several vulnerabilities that are specific to the healthcare sector:

1. Data Sensitivity and Volume:

Healthcare organizations store vast amounts of sensitive data, including patient

health records, financial information, and personal identifiers. These data are highly valuable on the black market, making healthcare a prime target for cybercriminals (Martin et al., 2017). The 2015 Anthem breach, where 80 million records were stolen, underscores the lucrative nature of healthcare data. These individual medical records are valued at around 50\$ on the dark web, which would make this breach have a market value of over a billion dollars. (Martin et al., 2017)(Hoffman, 2020).

2. Legacy Systems and Outdated Software:

Healthcare institutions often rely on outdated and unsupported systems, creating significant cybersecurity vulnerabilities. Legacy client operating systems, such as Windows XP or Windows 7, and server operating systems such as Windows Server 2008, lack critical security updates and remain susceptible to well-documented exploits. (Martin et al., 2017). Illustratively, the WannaCry ransomware attack, which affected numerous hospitals worldwide, exploited vulnerabilities in outdated operating systems (Kaspersky, 2024).

Beyond operating systems, outdated database software like Oracle 12c and SQL Server 2008 remain in use in some healthcare settings, despite no longer receiving security patches or updates. These systems often fail to meet modern encryption and security standards, exposing sensitive patient data to unauthorized access. Similarly, older web browsers, such as Internet Explorer, are vulnerable to modern phishing attacks and malware, further compounding the risks.

3. Fragmented Governance and Limited Resources:

The governance structure within healthcare is often fragmented, leading to unclear accountability and inconsistent security measures. Additionally, healthcare organizations frequently face budget constraints that limit their ability to invest in robust cybersecurity defenses (Martin et al., 2017). This combination of fragmented governance and limited resources exacerbates the sector's vulnerability to cyberattacks.

4. Increased Attack Surface Due to Digitalization:

The digitalization of healthcare services has increased the attack surface for cybercriminals. The integration of Internet of Things (IoT) devices, such as wearable health monitors and connected medical equipment, introduces new entry points for attacks. These devices often lack adequate security features, making them easy targets for hackers (Javaid, Haleem, Singh, & Suman, 2023).

5. Human Factors and Insider Threats:

Human error remains one of the most significant vulnerabilities in cybersecurity (see Figure 6), particularly in the healthcare sector. Studies show that a large proportion of ransomware and phishing attacks are successful because employees inadvertently

enable these threats, often by clicking malicious links or sharing sensitive information due to phishing emails (McLeod & Dolezel, 2018). Healthcare organizations, with their complex operational workflows, interconnectedness of systems, and limited cybersecurity awareness compared to other sectors, are especially susceptible to such errors. According to Kruse et al. (2017), insufficient training and a lack of awareness about cybersecurity best practices further increases this vulnerability, leaving institutions open to exploitation.

6. High Dependence on Third-Party Vendors:

Healthcare providers often rely on third-party vendors for various services, from IT support to medical equipment maintenance. These vendors may not adhere to the same security standards, or require complicated and costly system upgrades, creating additional vulnerabilities (Chigada & Madzinga, 2021). The interconnected nature of healthcare systems means that a breach from one vendor or system component can have cascading effects on the entire network.

3.3 Economic magnitude of ransomware attacks on the healthcare sector

The economic impact of ransomware attacks on the healthcare sector has multiple sides, affecting not only the financial stability of healthcare institutions but also patient care, regulatory compliance, and overall healthcare delivery. In this chapter the literature on the financial consequences of ransomware attacks on healthcare organizations is analyzed, with a focus on both direct and indirect costs, following the methodology of Anderson et al. (2013), as well as long-term financial implications. Their approach decomposes the cost of cybersecurity attacks into three categories: defense costs, direct costs and indirect costs.

Direct costs

Ransomware attacks result in substantial direct financial costs for healthcare organizations. These costs include ransom payments, expenses associated with system restoration, and legal fees. According to IBM's "Cost of a Data Breach Report 2024", the average cost of a data breach in the healthcare sector is significantly higher than in other industries, averaging \$9.77 million per incident (IBM, 2024), compared to the global industry average of \$4.88 million. This figure is composed of immediate response costs and long-term expenses related to data breaches. Despite a 10% decrease in average breach cost since 2023, the healthcare industry remains the top costliest industry for breaches since 2011.

The ransom payments themselves can vary widely depending on the size and type of

institution as well as the extent of the compromised systems and data. For example, the Hollywood Presbyterian Medical Center (HPMC), a small private acute care facility, paid \$17 000 in Bitcoin to regain access to their systems after a ransomware attack in 2016 (Martin et al., 2017). In contrast, the smaller Saint-Luc hospital in Bouge paid €150 000 in ransom following the attack in 2021. This increase reflects the growing sophistication of ransomware attacks and the higher valuation of critical healthcare data over time, and the Saint-Luc attack highlights how even smaller institutions are increasingly targeted with higher demands. While HPMC is larger in bed count (430 vs 302), the Saint-Luc Bouge hospital operates in an interconnected digital ecosystem, where even localized disruptions can have far-reaching financial consequences.

However, these ransom payments are just a fraction of the total costs. Other significant expenses include system downtime and the costs of recovering and restoring data. For example, the WannaCry ransomware attack caused significant disruption and financial loss across the UK's National Health Service (NHS), where the total cost was estimated at £92 million, £20 million from lost output, and £72 million from the IT support to recover from the attack (NHE, 2018).

Indirect costs

Indirect costs of ransomware attacks include lost revenue due to operational disruptions, decreased patient trust, and the long-term financial impact of reputational damage. Operational disruptions caused by ransomware can be severe. For instance, the WannaCry attack led to widespread disruption in the UK's NHS, causing appointment cancellations and delayed treatments, which consequently affected revenue and patient outcomes (Martin et al., 2017). These disruptions can result in significant revenue loss due to canceled procedures, treatments, and diverted emergency services.

Moreover, ransomware attacks can lead to substantial legal and regulatory costs. Healthcare organizations are subject to strict data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union. Non-compliance or breaches of these regulations can result in hefty fines. In especially severe cases, the GDPR allows for fines up to €20 million or 4% of annual global turnover, whichever is higher (GDPR-info.eu, n.d.).

Defense costs

In addition to direct and indirect costs, defense costs represent a significant economic burden for the healthcare sector in its efforts to mitigate ransomware attacks. These costs encompass investments in cybersecurity infrastructure such as firewalls, endpoint

protection, network segmentation, and staff training programs to reduce susceptibility to phishing and social engineering attacks (IBM, 2024). For instance, global spending on cybersecurity in the healthcare sector amounted to over 16 billion euros in 2023, with forecasts projecting it to surpass 25 billion euros by 2026, growing at a compound annual growth rate of 14%, the highest rate across all industries (Yang, 2023). Hospitals often allocate substantial budgets to real-time threat monitoring and incident response systems, with many outsourcing these functions to specialized cybersecurity firms to compensate for in-house expertise gaps (Kolade et al., 2023). In Belgian hospitals, this is further complicated by fragmented governance structures and constrained budgets, which limit the ability to implement comprehensive defenses. Including defense costs in the analysis underscores the importance of proactive strategies, such as endpoint detection systems and staff education, to enhance resilience while controlling the growing financial burden of cybersecurity investments.

Case Study: economic impact analysis

Portela et al. (2023) conducted a detailed case study on the economic impact of cyberattacks on the national healthcare system in Portugal. The study found that the immediate costs included expenses for IT support and system restoration, while long-term costs encompassed regulatory fines, legal fees, and investments in improved cybersecurity measures to prevent future incidents. The total economic impact was estimated to range from €115 882.96 to €2 317 659.11 depending on the amount of disrupted working days and affected resources (Portela, Nogueira-Leite, Almeida, & Cruz-Correia, 2023). The study considers a maximum of 5 disrupted working days to calculate the estimated cost, but as explained by Pierre Colin, the CIO of the Saint-Luc Hospital in Brussels, the interruptions could last up to several weeks in extreme cases, meaning the costs could go amount to even higher sums. This clearly shows the immense financial burden of such attacks for a hospital.

Breakdown of ransomware attack costs

To provide a clearer understanding of the financial implications, the table below outlines the various cost categories associated with a ransomware attack, and their estimated cost according to the different studies:

Cost Category	Description	Estimated Cost
Ransom Payment	Direct payment to attackers to regain access to data	\$17,000 (Martin et al., 2017)
System Restoration	Costs of restoring IT systems and recovering data	\$500,000 - \$2,000,000 (P. I. IBM, 2023)
Operational Disruptions	Lost revenue due to system downtime and canceled appointments	\$1,000,000 - \$5,000,000 (NHE, 2018)
Legal and Regulatory Fees	Fines, legal fees, and compliance costs	Up to €20 million or 4% of annual turnover (GDPR-info.eu, n.d.)
Reputational Damage	Long-term revenue loss due to decreased patient trust	Variable (Portela et al., 2023)
Cybersecurity Improvements	Investments in IT infrastructure and training to prevent future attacks	\$1,000,000 - \$3,000,000 (P. I. IBM, 2023)

Table 2: Estimated costs associated with ransomware attacks on healthcare organizations

However, it is important to keep in mind that the financial impact these ransomware attacks cause on healthcare institutions can be highly variable, influenced by factors such as the size of the institution, the centralization of its systems, and the scope of the attack. Larger institutions, like university hospitals, often face higher absolute costs due to their broader reliance and centralization of digital infrastructure. For example, a large hospital with a massive, single electronic health record (EHR) system, could experience significant operational disruptions if the system is entirely disabled during an attack, as seen in previous incidents (Smith, 2018). Conversely, smaller healthcare facilities with limited budgets often face disproportionate challenges in recovering from such incidents, as their capacity for implementing robust cybersecurity measures is inherently constrained by budgets (Meisner, 2018).

Ransomware costs have also increased significantly in recent years. In the 2016 attack on Hollywood Presbyterian Medical Center, the ransom was \$17,000, while recovery costs in similar incidents now often exceed €1 million (Martin et al., 2017). In their 2024 study analyzing the cost of a databreach, IBM estimates an average cost of \$9.77 million for healthcare data breaches globally, reflecting increased dependency on digital systems and more sophisticated attack techniques (IBM, 2024).

The financial consequences also depend on the extent of the attack. Smaller-scale in-

cidents, such as the 2022 Sint-Andriesziekenhuis malware attack, incurred minimal costs due to limited scope and effective containment (Sint-Andries Ziekenhuis, 2022). However, larger incidents, like the CHRSM ransomware attack, involved extensive data exfiltration and operational downtime of critical systems, with costs surpassing €3 million (Hennuy & Van Oppens, 2024).

3.4 Proactive risk mitigation strategies

As healthcare systems become increasingly digital, the need for robust cybersecurity measures becomes ever more critical. Proactive risk mitigation strategies are therefore essential in safeguarding the healthcare systems against the growing threat of cyberattacks. Implementing these strategies effectively can significantly reduce the risk of cyber incidents, minimize financial losses, and improve overall cybersecurity resilience within healthcare institutions.

3.5 Reactive vs proactive cybersecurity

But why proactive ? In the realm of cybersecurity, strategies can broadly be categorized as either reactive or proactive. In order for an organization to enhance its cybersecurity posture, it is vital to understand the difference between the two.

Reactive cybersecurity involves responding to incidents after they occur. Its characteristics are listed below:

- **Incident Response:**
Reactive strategies primarily focus on detecting and responding to cyber incidents post-occurrence. The goal is to mitigate the impact of the breach and restore normal operations as quickly as possible.
Reactive measures include activities such as incident response, forensic analysis, and remediation efforts aimed at addressing vulnerabilities exposed by the attack (Bhuyan et al., 2020).
- **Damage Control:**
The emphasis of reactive cybersecurity is on damage control and recovery. This includes identifying the breach, assessing the extent of damage, and taking steps to contain and remediate the impact. As described by Katsumata et al. (2010), this approach often leads to significant downtime and operational disruptions whilst organizations struggle to respond to the attack.
- **Post-Event Analysis:**
Reactive cybersecurity involves analyzing the breach after it has occurred to understand how it happened and what measures can be taken to prevent future incidents.

In their study, Kwon and Johnson (2014) highlight that this can lead to improved defenses, but only after suffering the consequences of the initial attack.

- **Cyber Insurance:**

Cyber insurance provides financial protection by covering costs related to ransomware incidents, such as ransom payments, data recovery, and legal fees. While it does not prevent attacks, it serves as a safety net for mitigating financial losses (Bhuyan et al., 2020).

Proactive cybersecurity, on the other hand, involves anticipating and mitigating threats before they can cause harm. This approach focuses on the following aspects:

- **Threat Prevention:**

Proactive strategies focus on preventing cyber incidents through continuous monitoring, threat intelligence, and risk assessments. The goal is to identify and neutralize threats before they can exploit vulnerabilities. Bhuyan et al. (2020) stress that transitioning to proactive cybersecurity involves keeping systems patched and up-to-date, deploying advanced technologies such as firewalls, intrusion detection and prevention systems (IDPS), encryption, and multi-factor authentication (MFA) to detect and mitigate threats early.

- **Continuous Improvement:**

Furthermore, this strategy involves regularly updating and improving security measures based on the latest threat intelligence and vulnerability assessments. Maintaining up-to-date software and systems, and implementing automated patch management is thus very important to reduce the risk of exploitation (Cremer et al., 2022).

- **Security Awareness and Training:**

A proactive approach also includes ongoing training and awareness programs for employees to ensure they are well-versed in cybersecurity best practices and can recognize potential threats. According to Alanazi (2023), fostering a culture of security through regular training and simulations is essential for preventing human errors that could lead to security breaches.

- **Strategic Planning and Governance:**

Lastly, proactive cybersecurity requires strong governance structures and strategic planning to ensure that security measures are integrated into every aspect of the organization's operations. A good practical implementation can be found in the study from Goel et al. (2020), in which they describe the PRISM framework, which helps organizations make strategic decisions about cybersecurity investments, ensuring that resources are allocated effectively to mitigate risks.

The table below summarizes the key differences between reactive and proactive cybersecurity approaches:

	Reactive Cybersecurity	Proactive Cybersecurity
Focus	Responding to incidents post-occurrence	Preventing incidents before they occur
Primary Activities	Incident response, forensic analysis, damage control	Continuous monitoring, threat intelligence, risk assessments
Technology Use	Basic security tools, post-event analysis tools	Advanced security technologies (updating systems, firewalls, IDPS, encryption, MFA)
Operational Impact	High downtime and disruption during incident response	Minimal disruption with continuous protection and prevention
Employee Role	Limited to incident response roles	Active participation in training, awareness programs, and simulations
Governance	Ad-hoc and reactive governance	Strategic and integrated governance with continuous improvement

Table 3: Comparison of reactive and proactive cybersecurity approaches

Clearly, understanding the distinctions between reactive and proactive cybersecurity is crucial for healthcare organizations.

Earlier research indicated that a reactive strategy is more cost effective than a proactive one since uncertainty about the "weakest link" may lead to overinvestment when adopting a proactive risk mitigation strategy (Rowe & Gallaher, 2006). However, considering that the healthcare industry is lagging behind other industries in terms of cybersecurity, yet handles highly confidential, critical data that is often being targeted, the uncertainty over where to invest is significantly lower.

The ENISA 2023 report underscores that ransomware attacks in healthcare mostly target patient records, because it is a highly lucrative asset for cybercriminals. Therefore, proactive defense measures, such as encryption and training programs, are highly recommended since according to the ENISA they can reduce the probability of data breaches by more than 50% (European Union Agency for Cybersecurity, 2023).

By **shifting towards a proactive approach**, and investing in their well-known weaknesses, the healthcare sector could thus significantly reduce the risk of cyberattacks and improve their overall resilience and cost-effectiveness. (Kwon & Johnson, 2014; Kolade et

al., 2023)

3.6 Conclusion

The literature reviewed highlights a clear consensus among experts and sources: the healthcare sector faces unique and significant cybersecurity challenges due to its particular ecosystem, having to rely on thousands of interconnected systems, sensitive patient data, and often outdated technologies. Studies consistently point to a troubling gap between the sector's digital dependency and its preparedness to address evolving cyber threats. The healthcare sector's vulnerabilities are first and foremost due to constrained budgets, but also fragmented governance and legacy systems, making it an attractive target for ransomware and other cyberattacks.

Despite these challenges, there is broad agreement that proactive risk mitigation strategies are essential to improving cybersecurity resilience. The adoption of frameworks like the NIS2 Directive and increasing collaboration between healthcare institutions, policymakers, and cybersecurity experts reflect a growing awareness of the urgency of these issues. However, the slow pace of change and the rising sophistication of cyber threats indicate that significant work remains to be done.

4 Analysis of the impact a ransomware attack on a Belgian hospital

The objective of this section is to examine the impact of a ransomware attacks on Belgian hospitals, using the Centre Hospitalier Sambre-Meuse (CHRSM) as a case study. The analysis focuses on the financial, operational, and long-term repercussions of a ransomware attack on a large healthcare institution.

4.1 Analysis of the economic impact of ransomware attacks on the Belgian healthcare sector

Ransomware attacks have emerged as a significant threat to the healthcare sector globally, with Belgium being no exception. The increasing digitization of healthcare services, while enhancing patient care and operational efficiency, has also expanded the attack surface for cybercriminals. The economic impact of these attacks on Belgian healthcare institutions can be categorized into direct financial losses, operational disruptions, and indirect costs.

Direct financial losses

Direct financial losses from ransomware attacks include ransom payments, costs associated with system restoration, and investments in cybersecurity measures post-incident. For instance, the Vivalia Hospital Group in Belgium experienced a ransomware attack in May 2022 that disrupted all services, with partial recovery taking up to seven weeks. The estimated costs for operational disruptions and recovery exceeded €3 million.

Similarly, the CHR Sambre et Meuse (CHRSM) faced a ransomware attack in May 2023, resulting in the theft of 127 GB of data and severe disruption of critical services. The financial implications were significant, with estimated costs ranging between €1 million and €2 million, encompassing data recovery efforts and operational losses.

Operational disruptions

Operational disruptions caused by ransomware attacks can be severe, affecting patient care and hospital workflows. The CHwapi hospital in Tournai experienced a ransomware attack in January 2021 that disabled 80 servers, leading to the redirection of emergency services and delayed operations. Such disruptions not only impede healthcare delivery but also decrease patient trust in the affected institutions.

The Sint-Andriesziekenhuis in Tielst detected malware on one server in January 2022. Their swift action prevented significant operational impact, and no confidential data was

exposed in the end. This incident underscores the importance of rapid response in mitigating potential disruptions and financial losses.

Indirect costs

Indirect costs include reputational damage, loss of patient trust, legal fees, and potential regulatory fines. While specific figures for Belgian hospitals are not always disclosed, the global healthcare sector has witnessed substantial indirect costs due to ransomware attacks. For example, a ransomware attack on Universal Health Services in the United States resulted in an estimated economic impact of \$67 million, highlighting the potential scale of indirect costs (Kolbasuc McGee, 2021).

In Belgium, the unauthorized access to internal documents at AZ Herentals in April 2022, although not compromising patient records, likely led to indirect costs related to patient notification and compliance measures. Such incidents can diminish public confidence and necessitate investments in public relations efforts to restore trust.

4.2 Quantitative data on financial losses, recovery costs, and indirect costs

The table below gives an overview of the financial and operational impacts of ransomware on Belgian healthcare facilities, using cases that have been explored earlier in this thesis.

Table 4: Summary of financial and operational impacts of ransomware attacks on Belgian healthcare institutions

Date	Institution	Type of Attack	Direct Costs	Operational Disruptions	Indirect Costs
Jan 2021	CHwapi, Tournai	Ransomware	€1M+	80 servers disabled, emergency services redirected, delayed operations	Reputational damage, potential legal fees
Jan 2022	Sint-Andriesziekenhuis, Tielt	Malware	Minimal	Malware detected on one server; swiftly mitigated. No confidential data exposed	Negligible
Apr 2022	AZ Herentals	Data Breach	Not disclosed	Unauthorized access to internal documents. Patient records not compromised	Patient notification, compliance measures
May 2022	Vivalia Hospital Group	Ransomware	€3M+	Disrupted all services, partial recovery after 7 weeks	Reputational damage, loss of patient trust
May 2023	CHR Sambre et Meuse (CHRSMB)	Ransomware	€3M-€5M	127 GB data stolen, critical services severely disrupted	Legal fees, compliance costs

We have already established that globally, the healthcare sector has been increasingly targeted by ransomware attacks. In 2023 alone, the American healthcare sector reported 249 ransomware attacks to the FBI, making it the most targeted industry (HealthManagement.org, 2024a). These attacks have led to significant operational disruptions, including delayed patient care and compromised safety.

With regards to our own continent, the ENISA reported that ransomware attacks accounts for 54% of cybersecurity threats in the health sector (European Union Agency for Cybersecurity, 2023). The increasing frequency and sophistication of these attacks underscore the urgent need for enhanced cybersecurity measures within healthcare institutions.

To get a better grasp on the precise financial implications for a Belgian hospital, the following table analyses the recent attack on the Centre Hospitalier Sambre-Meuse (CHRSM) to fully decompose the various financial consequences of a ransomware attack on a hospital. The cost types and descriptions are based on Meisner (2018)'s similar research on a Polish public hospital.

For context, here are some key numbers regarding the CHRSM, mostly found on their website:

- Bed Capacity: The hospital has approximately 700 licensed beds.
- Staff: CHRSM employs over 3,000 staff members, including 380 physicians.
- Patient Services: Around 278 000 consultations annually, more than 56 000 emergency department visits per year, and about 2200 births each year.
- Turnover in 2023: €307 148 392,60 (National Bank of Belgium, 2023)

Table 5: Analysis of the estimated cost of the ransomware attack on the CHRSM

Type of Costs	Description	Estimated Cost (€)
Forensic Investigation	Engaging external cybersecurity experts for 3 weeks (5 experts working 8h/day at €200/hour).	120 000
Breach Notification	Notification costs for 10 000 affected patients at €10 each.	100 000
Post-Breach Protection	Offering identity theft protection (€15 per patient, 10% uptake by affected individuals).	15 000
Litigation and Regulatory Fines	Legal defense (€150 000), settlement (€250 000), and GDPR-related fines (up to €2 million).	2 400 000
Cybersecurity Enhancements	Upgrading systems to address vulnerabilities identified during the breach.	500,000
Loss of Reputation and Patient Churn	The attacked hospital was public healthcare provider and probably suffered of loss of reputation, no information on patient churn ^a	-
Operational Downtime	Estimated daily operational losses (€136 986,30/day) over 10 days of significant downtime.	1 369 863
Data recovery and IT Restoration	Efforts to restore stolen and encrypted data, including reinstalling systems and backups (€50 000/day for 10 days)	500 000
Total Estimated Cost		5 004 863

^apatient churn is the phenomenon where a dissatisfied patient cancels their appointment or chooses another healthcare provider over your organization

The total estimated cost of the ransomware attack on the CHR Sambre & Meuse was publicly announced to be somewhere between 3 and 5 million euros.(Hennuy & Van Op-pens, 2024), but this estimation in this work takes upper bounds of the cost into account.

4.3 Qualitative impact of ransomware attacks

The financial ramifications of ransomware in the healthcare sector are substantial, but the qualitative impacts are equally significant, affecting patient safety, operational continuity, institutional trust, and employee morale. Understanding these dimensions is essential to understand the full consequences of cyberattacks.

Patient safety and health outcomes

- **Delayed Care:** Ransomware attacks often result in delayed procedures and diagnostics, jeopardizing patient outcomes. For instance, during the CHwapi attack in 2021, 80 servers were disabled, leading to postponed surgeries and patient transfers.
- **Loss of Critical Information:** Attacks compromise access to Electronic Health Records (EHRs), making it difficult for healthcare providers to deliver informed care.
- **Mistrust:** Breaches involving sensitive personal and health data erode patient confidence, discouraging engagement with digital healthcare services.

Operational disruptions

- **Interruptions in Service Delivery:** Hospitals like Vivalia and CHRSM experienced prolonged recovery times, with services disrupted for weeks.
- **Shift to Manual Operations:** Institutions often revert to paper-based systems or individual workstation software during recovery, meaning they have no access to medical history and overall patient information. This increases the likelihood of human errors and further reduces efficiency.

Reputation and institutional trust

- **Public Perception:** Repeated incidents tarnish the reputation of healthcare institutions, affecting their ability to secure funding and attract talent.
- **Legal Repercussions:** Data breaches increase the risk of lawsuits, regulatory scrutiny, and fines, which can further harm institutional standing.

Workforce morale

- **Employee Stress:** IT staff and healthcare workers face significant pressure during cyber incidents, with extended hours required for system recovery and operational continuity, since cyberattacks often require going back to paper-based ordering, reporting, going back to acquisition consoles (e.g. for ECG's, medical image scans), etc.
- **Skill Gaps:** Lack of training in handling cyber crises exacerbates the burden on existing personnel, leading to potential burnout.

We can conclude from this section that ransomware attacks clearly impose substantial economic burdens on Belgian healthcare institutions, encompassing direct financial losses, operational disruptions, and indirect costs. The increasing frequency of these attacks highlights the critical need for robust cybersecurity strategies, especially proactive risk mitigation measures, to safeguard healthcare services and maintain public trust. Investments in cybersecurity help not only to protect sensitive patient data but also to ensure the continuity of essential healthcare services, thereby mitigating this multifaceted economic impacts of ransomware attacks.

5 Proactive Risk Mitigation Strategies

The increasing appearance of ransomware attacks on healthcare institutions has emphasized the critical need for effective cybersecurity strategies. Belgian hospitals, as part of the broader European healthcare ecosystem, have adopted several proactive risk mitigation strategies to prevent and minimize the impact of cyberattacks. This section identifies the strategies currently in use, evaluates their effectiveness in reducing financial losses, and highlights successful case studies from Belgian healthcare institutions.

5.1 Identification and evaluation of proactive risk mitigation strategies currently in use in the Belgian healthcare sector

Belgian hospitals have recently been implementing various strategies to enhance their resilience against cyberattacks, but often as a reaction to falling victim of one. The following approaches are commonly observed:

Incident Response Plans:

Hospitals are adopting detailed incident response protocols to handle ransomware attacks effectively. These plans include procedures for isolating affected systems, coordinating with external experts, and restoring operations. For example, CHR Sambre et Meuse (CHRSMB) updated its incident response protocols after the 2023 ransomware attack, which enables faster recovery during subsequent incidents.

Regular Data Backups:

Backup systems are critical in ensuring data restoration without paying a ransom. Many hospitals, including CHU Liège, have implemented redundant backup systems stored offline to avoid encryption by ransomware.

Cybersecurity Awareness Training:

Regular training programs aim to educate healthcare employees about recognizing phishing attempts and adhering to best practices. CHU Saint-Pierre observed a 30% reduction in phishing-related incidents after initiating awareness campaigns.

Similarly, Pierre Colin, CIO of the Saint-Luc Hospital in Brussels, described their use of an integrated application that sends simulated phishing emails to staff. Employees who fall for these fake phishing attempts are identified and required to undergo additional cybersecurity training. The tool offers training programs and allows the hospital to follow up on who underwent training, and see their progress in personnel awareness on a dashboard (P. Colin, personal communication, 05/07/2024). This targeted approach not only

enhances individual awareness but also strengthens the institution's overall cybersecurity posture by addressing vulnerabilities directly.

Network Segmentation:

Segmenting hospital networks helps limit the spread of ransomware by isolating infected systems. Sint-Andriesziekenhuis effectively contained malware to a single server during a 2022 attack due to its segmented architecture (Sint-Andries Ziekenhuis, 2022). However, due to budgetary reasons, this is a challenge for a lot of hospitals, to quote P. Colin, CIO of Saint-Luc's hospital in Brussels, *"If I have to segment the network in a way that makes the network adequately secured for a hospital, I think I have to hire two more persons. And I cannot, so this is one of the challenges we are facing."*

Multi-Factor Authentication (MFA):

Many institutions have adopted MFA to enhance security for remote access to sensitive systems, reducing unauthorized access risks. The Saint-Luc hospital in Brussels even goes a step further, applying a Zero-Trust Architecture². (P. Colin, personal communication, 05/07/2024).

Collaboration with External Cybersecurity Firms:

Hospitals more often than not engage third-party cybersecurity firms for real-time monitoring and threat intelligence due to lack of funds or personnel to maintain a proper cyberdefence themselves. For example, Vivalia partnered with external experts to strengthen its defenses after a ransomware attack in 2022 (Le Soir, 2022).

Implementation of the NIS2 Directive:

Belgian hospitals are obliged to align with the EU's NIS2 Directive, which mandates risk management, incident reporting, and resilience-building measures for critical infrastructure. However, with the means and the budget that they are given, this is often difficult to manage in a short timeframe (P. Colin, personal communication, 05/07/2024).

Keeping Systems Up-to-Date

Maintaining updated systems is crucial in mitigating cyber risks. Outdated software, such as Windows Server 2008 or Oracle 12c, lacks security patches, making it vulnerable to exploitation. High-profile attacks like WannaCry have demonstrated the consequences of

²ZTA is a comprehensive security framework that assumes no user or device should be trusted by default, even if it is inside the network perimeter. Trust is earned dynamically based on continuous verification and context

failing to patch systems, which allowed attackers to exploit known vulnerabilities. Belgian hospitals can reduce these risks by implementing robust patch management practices, prioritizing updates for critical systems, and isolating outdated systems through network segmentation if updates are not feasible.

The American Cybersecurity & Infrastructure Security Agency (CISA, www.cisa.gov) registers and publishes any known cybersecurity vulnerability for all critical infrastructure, which includes hospital systems. Although it is an American government institution, it is typically leveraged throughout the world as the risks and applications in use are similar across the world. All software vendors proactively publish critical vulnerability disclosures related to their software applications, the level of risk, as well as possible mitigations (CISA, 2024).

5.2 Analysis of the effectiveness of these strategies in minimizing financial losses

The implementation of proactive cybersecurity measures has shown tangible benefits in reducing the financial and operational impacts of ransomware attacks in several cases illustrated in the table below:

Table 6: Effectiveness of proactive risk mitigation strategies in minimizing financial losses

Strategy	Effectiveness in Minimizing Financial Losses
Incident Response Plans	Reduced downtime and faster containment. CHRSM reported a 40% reduction in recovery time post-implementation.
Regular Data Backups	Eliminates the need for ransom payments and ensures data recovery. CHU Liège restored critical operations within days using backups.
Cybersecurity Awareness Training	Improved phishing detection reduced successful attack rates, as seen at CHU Saint-Pierre (30% reduction).
Network Segmentation	Contained malware to a single server, as demonstrated by Sint-Andriesziekenhuis.
Multi-Factor Authentication (MFA)	Prevented unauthorized access to sensitive systems, widely regarded as a cost-effective solution.
Collaboration with Cybersecurity Firms	Enhanced threat detection and response. Vivalia reported no major incidents in the year following their ransomware attack.

5.3 Case studies or examples of successful implementation of mitigation strategies

1. CHR Sambre et Meuse (CHRSM):

- After the May 2023 ransomware attack, CHRSM invested heavily in its cybersecurity framework, focusing on incident response planning and regular backups.
- Outcome: Recovery time decreased significantly, and the institution avoided ransom payments by leveraging offline backups

2. Vivalia Hospital Group:

- Vivalia suffered a severe ransomware attack that disrupted services for seven weeks. Following this incident, the hospital adopted MFA, strengthened network segmentation, and engaged cybersecurity experts.
- Outcome: Enhanced resilience and no significant incidents reported in the subsequent year.

3. CHU Liège:

- CHU Liège successfully defended against a large-scale cyberattack by relying on its pre-established incident response plans and redundant backup systems.
- Outcome: No critical services were disrupted, showcasing the importance of proactive preparation.

4. Sint-Andriesziekenhuis, Tiel:

- Detected and contained malware on a single server, demonstrating the effectiveness of network segmentation and rapid response measures.
- Outcome: Minimal operational disruption and no loss of confidential data

Proactive risk mitigation strategies, such as regular data backups, incident response planning, and network segmentation, are clearly proving essential in minimizing the financial and operational impacts of ransomware attacks on the Belgian healthcare sector. Case studies like those of Vivalia and CHR Sambre et Meuse highlight the tangible benefits of adopting these measures. However, challenges remain, particularly in the consistent implementation of such strategies across all institutions, in a proactive way rather than as a consequence of being attacked. As ransomware attacks grow in frequency and sophistication, continuous implementation and enhancement of these strategies are vital to safeguarding Belgian healthcare institutions.

6 Weighing Cyber Insurance vs. Improved Cybersecurity Practices

As previously discussed, proactive risk mitigation strategies are essential for reducing the likelihood and extent of cyberattacks. However, these measures often come with significant upfront and recurring costs, raising the question of whether healthcare institutions should also (or instead) invest in cyber insurance policies as a way to manage financial risks. Cyber insurance policies offer an alternative approach, shifting the financial burden of attacks to the insurers while leaving the question of prevention largely to the institution.

Healthcare organizations should therefore carefully evaluate the balance between proactive investment in cybersecurity and the financial protection offered by cyber insurance, or consider a hybrid approach that leverages the benefits of both.

6.1 Costs and Risks of Cyber Insurance

Cyber insurance policies cover costs associated with ransomware incidents, such as data recovery, legal fees, and operational downtime. However, rising premiums reflect the increasing frequency and scale of cyberattacks, particularly in sectors like healthcare. For example, reports indicate double-digit increases in premiums across the board, with some industries experiencing spikes of up to 79% year-over-year in certain markets, as insurers demanded higher cybersecurity standards, such as implementing multi-factor authentication and regular backups, to mitigate their own risk exposure (Wilson, 2022; gao.gov, 2022).

While cyber insurance can provide financial relief, it does not address the underlying causes of vulnerability. Institutions relying heavily on insurance without adequately investing in proactive cybersecurity measures remain at risk of significant operational disruptions and reputational damage. Marotta et al. (2017) emphasize that organizations with robust defenses not only experience fewer attacks but also benefit from reduced insurance premiums and better policy terms.

Balancing Insurance and Proactive Practices

A combined approach that integrates cyber insurance with proactive risk mitigation strategies is often the most effective solution. Cyber insurance serves as a financial safety net, while proactive measures reduce the probability and impact of incidents. For example, hospitals that keep their systems up-to-date to avoid exploitable vulnerabilities and invest in endpoint detection systems, real-time threat monitoring, and network segmen-

tation can minimize the scope of attacks, thereby lowering insurance costs and ensuring operational resilience.

To summarize, there are a few key considerations regarding cyber insurance:

- **Proactive measures**, though costly initially, provide long-term savings by reducing incidents. **Cyber insurance**, while providing immediate financial coverage, incurs recurring premiums.
- Institutions with lower **risk tolerance** should prioritize a strong cybersecurity framework alongside insurance, while those with higher risk tolerance may rely more heavily on insurance.
- **Regulatory compliance** has to be kept in mind. With the NIS2 Directive mandating minimum cybersecurity standards, relying solely on insurance is increasingly untenable for Belgian healthcare institutions.

So in conclusion, by combining proactive strategies with financial safeguards such as cyber insurance, healthcare institutions can create a comprehensive risk management framework that minimizes both the likelihood and impact of cyberattacks.

7 Discussion

7.1 Interpretation of findings in the context of existing literature

The conducted analysis of ransomware’s economic and operational impacts on Belgian healthcare institutions reveals a consistent pattern of substantial direct costs and prolonged operational disruptions. These findings align with other studies, such as those by (Portela et al., 2023), which emphasized the multifaceted nature of ransomware impacts on healthcare systems. The approach of this thesis to estimate the financial losses incurred by the CHRSM following the ransomware attack is consistent with the publicly announced cost of €3-5 million, and aligns with global average costs of such incidents, which typically range from €1 to €5 million depending on the scope of the attack and the hospital’s size.

Qualitative impacts, such as reputational harm and reduced patient trust, are difficult to notice in the public hospitals analysed in this thesis, as there is not much data available, and some attacks are still relatively recent. However, as Bhuyan et al. (2020) argue, the intangible consequences of cyberattacks, such as patient hesitancy to engage with digital healthcare platforms, often persist long after technical recovery. In the Belgian context, the frequency of attacks on hospitals like the CHRSM, CHwapi, and Vivalia underscores the urgent need for better preparation and response strategies to prevent serious reputational consequences.

7.2 Comparison with other sectors or countries if relevant

Belgium’s healthcare sector clearly faces significant cybersecurity challenges, particularly when compared to other critical infrastructure sectors like finance and energy. Financial institutions often exhibit higher cybersecurity maturity, characterized by substantial budgets and more robust incident response mechanisms. This disparity is largely due to strict regulatory requirements tailored to the financial sector, such as the Baseline Principles for Managing Cyber Security Risk developed by the Belgian Financial Services and Markets Authority (FSMA) in collaboration with the Centre for Cybersecurity Belgium (CCB)(Nauwelaerts, 2024) or the DORA (Digital Operational Resilience Act) Regulation, but also due to a difference in ecosystems.

In contrast, the healthcare sector has been slower to adopt comprehensive cybersecurity measures. A 2024 study by KLAS Research highlighted that while healthcare organizations demonstrate maturity in incident response, they remain largely reactive rather than proactive in risk management, especially concerning supply chain and asset management

(HealthManagement.org, 2024b).

This reactive posture leaves healthcare institutions vulnerable to cyber threats, including ransomware attacks that can disrupt patient care and compromise sensitive data.

Internationally, countries like the Netherlands have made significant strides in enhancing cybersecurity resilience through the implementation of the NIS2 Directive. The Dutch government has been proactive in transposing NIS2 into national legislation via the Cybersecurity Act (Cyberbeveiligingswet), anticipated to come into force in 2025 (van den Bosch & Steenbruggen, 2024). This legislative framework imposes cyber resilience obligations on essential entities, including healthcare organizations, thereby strengthening their cybersecurity posture.

Belgium has recently also taken steps to enhance cybersecurity across various sectors. The Belgian Act of 26 April 2024 establishes a framework for the cybersecurity of network and information systems of general interest for public security, transposing the NIS2 Directive into Belgian law (Bruyndonckx, 2024).

7.3 Implications for policymakers, healthcare administrators, and IT managers

The findings of this thesis underscore the critical need for a coordinated and practical approach to address the growing threat of ransomware attacks in the Belgian healthcare sector. Below are actionable recommendations tailored to policymakers, healthcare administrators, and IT professionals, with a focus on leveraging existing resources and practical strategies.

Policymakers

1. **Leverage National and International Resources:** Policymakers should promote and support collaboration with organizations such as **CERT.be**, Belgium's Computer Emergency Response Team, which provides real-time updates, threat intelligence, and incident response guidance.
2. **Mandate Cybersecurity Standards:** Establish enforceable minimum cybersecurity standards for healthcare institutions, similar to the NIS2 Directive, to ensure consistent baseline protections. These standards should include mandatory penetration testing and audits.
3. **Funding and Incentives:** Allocate dedicated budgets for public hospitals to invest in cybersecurity infrastructure and staff training. Consider offering financial

incentives, such as tax breaks or grants, for healthcare institutions that adopt robust cybersecurity practices.

Healthcare Administrators

1. **Utilize CERT.be Tools and Training:** Healthcare administrators can collaborate with **CERT.be** to conduct sector-specific risk assessments and participate in their cybersecurity training programs. CERT.be also provides incident response templates that hospitals can customize and implement.
2. **Adopt Real-Time Threat Intelligence Platforms:** Implement platforms like the MISP Threat Intelligence Sharing Platform (<https://www.misp-project.org>) to enable proactive sharing of cybersecurity threats across Belgian hospitals and healthcare institutions. This reduces response times and minimizes the risk of widespread attacks.
3. **Simulated Phishing Campaigns:** As highlighted in the interview with Pierre Colin, use phishing simulation tools to regularly test and improve employee awareness. These tools not only identify vulnerable staff but also provide targeted training to address specific weaknesses.
4. **Deploy a Security Operations Center (SOC):** Following the example of Saint-Luc Hospital, healthcare administrators should consider deploying a Security Operations Center (SOC) equipped with a Security Information and Event Management (SIEM) system. This system collects and centralizes security-related data from critical systems, such as firewalls, antivirus software, and Active Directory. With automated correlation algorithms, it detects abnormal security events and alerts the SOC team, which operates 24/7. For institutions lacking large internal teams, outsourcing SOC operations to specialized firms can provide continuous monitoring and rapid response to intrusions or anomalies.
5. **Develop a Cybersecurity Incident Response Plan:** Ensure a clear and well-practiced plan is in place for responding to ransomware incidents. Include steps for isolating affected systems, communicating with patients and staff, and restoring services quickly.

IT Professionals

1. **Access CISA's "#StopRansomware Guide":** IT professionals could refer to **CISA.gov**'s comprehensive ransomware guide, which provides detailed instructions on preparing for, responding to, and recovering from ransomware attacks. The guide also includes a checklist for securing networks and endpoints.

2. **Enhance Monitoring with Free Tools:** Use free tools like **CISA's Vulnerability Scanning Service** to proactively identify and mitigate vulnerabilities in hospital networks.
3. **Implement Multi-Layered Defenses:** Strengthening security with multi-factor authentication, network segmentation, and endpoint detection and response systems. Tools like **Cisco Umbrella** can also help prevent malware infections and block malicious DNS requests.
4. **Participate in Cybersecurity Exercises:** Join initiatives such as **CERT.be's** Cyber Exercises, which simulate real-world attack scenarios and help institutions prepare for emergencies. Collaborating with other institutions during these exercises also fosters a shared understanding of best practices.

Essentially, a unified approach involving all stakeholders is essential to combat the rising threat of ransomware. Policymakers should ensure sufficient funding and enforce standards, healthcare administrators must integrate cybersecurity into organizational culture, and IT professionals should employ adequate tools and strategies to protect systems. Together, leveraging existing resources like **CERT.be** and **CISA.gov**, Belgian healthcare institutions can strengthen their resilience and ensure uninterrupted care for patients.

8 Conclusion and Recommendations

This thesis has explored the economic impact of ransomware attacks on the Belgian healthcare sector, highlighting both the quantitative and qualitative repercussions. Through an analysis of financial losses, operational disruptions, and indirect costs, the aim was to illustrate the profound vulnerability of healthcare institutions in the face of evolving cyber threats.

The findings reveal that ransomware attacks not only impose significant financial burdens but also jeopardize patient safety and institutional trust. Belgian hospitals, designated as critical infrastructure, face unique challenges due to massive interconnectedness of systems, budgetary constraints, and a reactive cybersecurity culture. However, this thesis also underscores the tangible benefits of proactive risk mitigation strategies, like incident response planning, regular backups, and network segmentation, in reducing the severity of these impacts.

The current healthcare landscape in Belgium is forcing hospitals to consolidate into larger enterprises (for example AZORG merging two major hospitals in Aalst (Aneca, 2023), or ZAS merging the two major hospital networks in Antwerp (Joris, 2024)), which also implies consolidating IT systems. This means that the scale and extent of risks incurred by cyber attacks will inevitably grow in the coming years.

8.1 Recommendations for improving cybersecurity resilience in the Belgian healthcare sector

Building upon the findings, the following recommendations are proposed:

Policy and Governance Enhancements: Policymakers should ensure the comprehensive implementation of the NIS2 Directive in Belgium, coupled with financial incentives to support hospitals in meeting these obligations. A centralized cybersecurity agency focused on healthcare could provide guidance, monitoring, and coordinated responses.

Investment in Cybersecurity: Hospitals should prioritize the allocation of resources for cybersecurity measures such as multi-factor authentication, real-time threat detection systems, keeping systems up-to-date and robust backup solutions. These investments should be viewed as essential to protecting critical infrastructure rather than optional expenditures.

Staff Training and Awareness: Regular training for hospital staff on cybersecurity best practices is vital. Awareness campaigns and simulated phishing exercises can significantly reduce human errors, which are often exploited and the primary entry point for ransomware attacks.

Collaborative Efforts: Partnerships between healthcare institutions, cybersecurity experts, and governmental bodies could facilitate the sharing of threat intelligence and best practices, strengthening the sector's collective resilience.

8.2 Limitations and future research

This thesis is the result of several months of intensive reading, research, and analysis. While it achieves its objective of presenting an overview of the impact of ransomware on the Belgian healthcare sector, certain limitations remain, offering opportunities for future research. The qualitative research with IT professionals within the healthcare sector led to certain limitations, as engaging with the relevant stakeholders proved to be quite difficult, which could be explained by the sensitive nature of the subject. Furthermore, due to the complexity of the problem, this subject could benefit from further investigation, supported by more extensive resources and time.

Future research could aim to examine the long-term implications of ransomware attacks on patient trust and institutional reputation, as these qualitative aspects extend beyond immediate recovery and impact the broader societal perception of healthcare institutions. Additionally, further exploration into technologies such as artificial intelligence and blockchain, could uncover innovative approaches to strengthening cybersecurity defenses in healthcare settings, particularly in preventing and mitigating cyber threats. In IBM's 2024 study the impact of AI and machine learning to help improve cybersecurity resilience and reduce financial consequences proved to be pretty substantial, being the second best factor in mitigating average data breach cost (as can be seen in figure 4) (IBM, 2024).

A comparative analysis of cybersecurity practices across different EU healthcare systems would also provide an opportunity to identify best practices and areas for improvement, particularly in the context of implementing the NIS2 Directive. Furthermore, a focused investigation of the practical challenges of aligning Belgian hospitals with NIS2 requirements could result in realistic and actionable recommendations for policymakers and key stakeholders, ensuring more effective compliance and resilience across the sector.

To conclude, there are many ways future research can go to strengthen the knowledge on this subject. The shift towards a proactive risk mitigation mentality in the healthcare sector is the first of many steps that Belgian healthcare institutions will need to continue resisting the ever-increasing amount of cyberattacks.

References

- Alanazi, A. T. (2023, October). Clinicians' perspectives on healthcare cybersecurity and cyber threats. *Cureus*, 15(10), e47026. doi: 10.7759/cureus.47026
- Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., ... Savage, S. (2013). Measuring the cost of cybercrime. In R. Böhme (Ed.), *The economics of information security and privacy* (p. 265–300). Berlin, Heidelberg: Springer. Retrieved from https://doi.org/10.1007/978-3-642-39498-0_12 doi: 10.1007/978-3-642-39498-0_12
- Aneca, L. (2023, October). *Nieuw fusieziekenhuis in aalst zal azorg heten: “geven zorg van a tot z” | vrt nws: nieuws*. Retrieved from <https://www.vrt.be/vrtnws/nl/2023/10/16/a-zorg/>
- AZ Herentals. (2022). *Datalek in az herentals*. Retrieved from <https://www.azherentals.be/nieuws/datalek-in-az-herentals/>
- Belga. (2021, January). *Le centre hospitalier de tournai victime d'une cyberattaque*. Retrieved from <https://www.lalibre.be/regions/hainaut/2021/01/18/le-centre-hospitalier-de-tournai-victime-dune-cyberattaque-2M6HLWR24VGURNHF6IHU3QCWLY/>
- Belga. (2022a, April). *Datalek bij az herentals door cyberaanval*. Retrieved from https://www.gva.be/cnt/dmf20220420_94716955
- Belga. (2022b, May). *L'uliège et le chu de liège ont résisté à une vaste et longue cyberattaque*. Retrieved from <https://www.lesoir.be/444504/article/2022-05-25/luliege-et-le-chu-de-liege-ont-resiste-une-vaste-et-longue-cyberattaque>
- Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., ... Dobalian, A. (2020, May). Transforming healthcare cybersecurity from reactive to proactive: Current status and future recommendations. *Journal of Medical Systems*, 44(5), 98. doi: 10.1007/s10916-019-1507-y
- Bruyndonckx, B. (2024, October). *The implementation of the nis2 directive in belgium: enha...* Retrieved from https://www.lexgo.be/en/news-and-articles/13768-the-implementation-of-the-nis2-directive-in-belgium-enhancing-cybersecurity-resilience?utm_source=chatgpt.com
- Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during covid-19: A systematic literature review. *South African Journal of Information Management*, 23(1). Retrieved from <https://www.proquest.com/docview/2502108278/abstract/879B56A62E6740C7PQ/1> doi: 10.4102/sajim.v23i1.1277
- CHRSM. (2023, August). *Cyberattaque: Vol de données | chrsm.be*. Retrieved from <https://www.chrsm.be/cyberattaque>
- CISA. (2024). *Known exploited vulnerabilities catalog | cisa*. Retrieved from <https://>

- www.cisa.gov/known-exploited-vulnerabilities-catalog
- Clinique Saint-Luc Bouge. (2022, March). *Cyberattaque: rencontre avec le département informatique de la clinique*. Retrieved from <https://www.slbo.be/cyberattaque-rencontre-avec-le-departement-informatique-de-la-clinique/>
- Coveware. (2022, January). *Ransomware as a service: Innovation trends to watch*. Retrieved from <https://www.coveware.com/blog/2022/1/26/ransomware-as-a-service-innovation-curve>
- Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022, July). Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Papers on Risk Insurance*, 47(3), 698–736. doi: 10.1057/s41288-022-00266-6
- Curando. (2023a, January). *Curando door cyberaanval getroffen*. Retrieved from <https://www.curando.be/nieuws/curando-door-cyberaanval-getroffen>
- Curando. (2023b, January). *Update: Beperkte schade voor zorggroep curando na cyberaanval*. Retrieved from <https://www.curando.be/nieuws/update-beperkte-schade-voor-zorggroep-curando-na-cyberaanval>
- Digitale Toekomst. (2021, September). *Digitale toekomst | ziekenfonds oz getroffen door cyberaanval. welke 6 acties ondernam het na de hacking?* Retrieved from <https://www.digitaletoekomst.be/nl/cyber-security/nieuws/ziekenfonds-oz-getroffen-door-cyberaanval-6-acties-na-hacking>
- Douxfls, J. (2021, October). *La clinique saint-luc à bouge otage d'un piratage: 150.000€ réclamés par les hackers - la libre*. Retrieved from <https://www.lalibre.be/regions/namur/2021/10/12/la-clinique-saint-luc-a-bouge-otage-dun-piratage-150000-reclames-par-les-hackers-PEQU34507FDOHAPMABUVF65QN4/>
- Durieux, S. (2023, March). *Retour à la normale au chu saint-pierre cible d'une cyberattaque*. Retrieved from <https://www.lesoir.be/500384/article/2023-03-11/retour-la-normale-au-chu-saint-pierre-cible-dune-cyberattaque>
- European Union Agency For Cybersecurity. (2022). Enisa threat landscape for ransomware attacks. Retrieved from <https://data.europa.eu/doi/10.2824/456263>
- European Union Agency for Cybersecurity. (2023). *Enisa threat landscape report: health sector (january 2021 to march 2023)*. LU: Publications Office. Retrieved from <https://data.europa.eu/doi/10.2824/163953>
- Fobe, G. (2023, June). *Cyberattaque au chrsm: des données médicales sur le dark web?* Retrieved from <https://www.rtbef.be/article/cyberattaque-au-chrsm-des-donnees-medicales-sur-le-dark-web-11215743>
- gao.gov. (2022, July). *Rising cyberthreats increase cyber insurance premiums while reducing availability | u.s. gao*. Retrieved from <https://www.gao.gov/blog/rising-cyberthreats-increase-cyber-insurance-premiums-while-reducing>

- availability
- GDPR-info.eu. (n.d.). *Gdpr fines / penalties*. Retrieved from <https://gdpr-info.eu/issues/fines-penalties/>
- Giot, M. (2022, September). *Victime d'une tentative de cyberattaque, le groupe santé chc ne prend plus les rendez-vous que par téléphone*. Retrieved from <https://www.rtbfb.be/article/victime-d-une-tentative-de-cyberattaque-le-groupe-sante-chc-ne-prend-plus-les-rendez-vous-que-par-telephone-11110055>
- Giot, M. (2023, February). *Tentative de cyberattaque: le chc montlégia toujours en "phase rouge"*. Retrieved from <https://www.rtbfb.be/article/tentative-de-cyberattaque-le-chc-montlegia-toujours-en-phase-rouge-11156444>
- Goel, R., Kumar, A., & Haddow, J. (2020, January). Prism: a strategic decision framework for cybersecurity risk assessment. *Information Computer Security*, 28(4), 591–625. doi: 10.1108/ICS-11-2018-0131
- HealthManagement.org. (2024a, October). *Cyberattacks' impact on patient care, safety and trust*. Retrieved from <https://healthmanagement.org/c/cybersecurity/News/cyberattacks-impact-on-patient-care-safety-and-trust>
- HealthManagement.org. (2024b, September). *Klas 2024 cybersecurity benchmark in healthcare*. Retrieved from <https://healthmanagement.org/c/healthmanagement/issuearticle/klas-2024-cybersecurity-benchmark-in-healthcare-1>
- Hennuy, J.-C., & Van Oppens, X. (2024, April). La cyberattaque contre le chr sambre meuse aura finalement coûté entre 3 et 5 millions d'euros. *RTBF*. Retrieved from <https://www.rtbfb.be/article/la-cyberattaque-contre-le-chr-sambre-meuse-aura-finalement-coute-entre-3-et-5-millions-d-euros-11364114>
- Heymans, P. (2021, September). *Hackers slaan toe bij ziekenfonds oz: "klantgegevens bekeken, maar medische gegevens waren veilig"*. Retrieved from <https://www.vrt.be/vrtnws/nl/2021/09/11/hacking-oz/>
- Hoffman, S. A. E. (2020, July). Cybersecurity threats in healthcare organizations: Exposing vulnerabilities in the healthcare information infrastructure. *World Libraries*, 24(11). Retrieved from <https://worldlibraries.dom.edu/index.php/worldlib/article/view/588>
- IBM. (2024). Cost of a data breach report 2024. Retrieved from <https://www.ibm.com/reports/data-breach>
- IBM, P. I. (2023, July). Cost of a data breach report 2023. Retrieved from <https://www.ibm.com/reports/data-breach>
- Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023, December). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, 1, 100016. doi: 10.1016/j.csa.2023.100016

- Joris, M. (2024, July). *Grootste ziekenhuis van het land wordt nog groter: fusie tussen zna en gza goedgekeurd*. Retrieved from <https://www.vrt.be/vrtnws/nl/2024/07/01/grootste-ziekenhuis-van-het-land-wordt-nog-groter-fusie-tussen/>
- Kaspersky. (2024, March). *What is wannacry ransomware ?* Retrieved from <https://www.kaspersky.com/resource-center/threats/ransomware-wannacry> (Last visited on 11/06/2024)
- Katsumata, P., Hemenway, J., & Gavins, W. (2010, October). Cybersecurity risk management. In *2010 - milcom 2010 military communications conference* (p. 890–895). San Jose, CA, USA: IEEE. Retrieved from <http://ieeexplore.ieee.org/document/5680181/> doi: 10.1109/MILCOM.2010.5680181
- Kirubavathi, G., Regis Anne, W., & Sridevi, U. K. (2024, November). A recent review of ransomware attacks on healthcare industries. *International Journal of System Assurance Engineering and Management*, 15(11), 5078–5096. doi: 10.1007/s13198-024-02496-4
- Kolade, A., Onunka, T., Daraojimba, C., Eyo-Udo, N., Onunka, O., Omotosho, A., & Okafor, C. (2023, October). Mitigating cybersecurity risks in the u.s. healthcare sector. , X, 177–194. doi: 10.51244/IJRSI.2023.10918
- Kolbasuc McGee, M. (2021, March). *Ransomware attack's economic impact: 67 million*. Retrieved from <https://www.bankinfosecurity.com/ransomware-attacks-economic-impact-67-million-a-16095>
- Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017, February). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, 25(1), 1–10. doi: 10.3233/THC-161263
- Kwon, J., & Johnson, M. E. (2014). Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly*, 38(2), 451–A3.
- Le Soir. (2022, May). *Attaque sur le réseau vivalia*. Retrieved from <https://www.lesoir.be/442643/article/2022-05-16/attaque-sur-le-reseau-vivalia-les-hopitaux-cibles-de-choix-des-cybercriminels>
- Louvigny, A. (2022, June). *Cyberattaque chez vivalia: sept semaines après, tous les secteurs n'ont pas redémarré*. Retrieved from <https://www.rtf.be/article/cyberattaque-chez-vivalia-sept-semaines-apres-tous-les-secteurs-n-ont-pas-redemarre-11021447>
- Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017, May). Cyber-insurance survey. *Computer Science Review*, 24, 35–61. doi: 10.1016/j.cosrev.2017.01.001
- Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017, July). Cybersecurity and healthcare: how safe are we? *BMJ*, j3179. doi: 10.1136/bmj.j3179
- McLeod, A., & Dolezel, D. (2018, April). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, 108, 57–68. doi: 10.1016/

- j.dss.2018.02.007
- Meisner, M. (2018, March). Financial consequences of cyber attacks leading to data breaches in healthcare sector. *Copernican Journal of Finance Accounting*, 6, 63. doi: 10.12775/CJFA.2017.017
- Montero, A., Mergen, S., & Wuidart, P. (2021, January). *Attaque informatique au chwapi: les opérations non urgentes reportées, les consultations maintenues*. Retrieved from <https://www.rtbef.be/article/attaque-informatique-au-chwapi-les-operations-non-urgentes-reportees-les-consultations-maintenues-10676223>
- Muslim, A. K., Mohd Dzulkifli, D. Z., Nadhim, M. H., & Abdellah, R. H. (2019, June). A study of ransomware attacks: Evolution and prevention. *Journal of Social Transformation and Regional Development*, 1(1). Retrieved from <https://publisher.uthm.edu.my/jstard/index.php/jstard/article/view/27/13> doi: 10.30880/jstard.2019.01.01.003
- National Bank of Belgium. (2023, December). *Bilan nbb chrsm*. Retrieved from <https://consult.cbso.nbb.be/consult-enterprise>
- Nauwelaerts, W. (2024, March). *Cybersecurity 2024 - belgium | global practice guides | chambers and partners*. Retrieved from <https://practiceguides.chambers.com/practice-guides/cybersecurity-2024/belgium>
- NHE. (2018, October). *Wannacry cyber-attack cost the nhs £92m after 19,000 appointments were cancelled*. Retrieved from <https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled>
- Noulet, J.-F. (2024, July). Cyberattaques: en belgique, les hôpitaux parmi les plus visés. *RTBF*. Retrieved from <https://www.rtbef.be/article/cyberattaques-en-belgique-les-hopitaux-parmi-les-plus-vises-11412417>
- Numerikare. (2022, June). " transformons la cyberattaque de vivalia en opportunité pour mieux protéger nos hôpitaux " (f.vandenbroucke). Retrieved from <https://www.numerikare.be/fr/actualites/transformons-la-cyberattaque-de-vivalia-en-opportunite-pour-mieux-proteger-nos-hopitaux-f-vandenbroucke.html>
- Poncelet, A. (2022, May). *Une attaque informatique contre l'université et le chu de liège pendant 26 heures. la situation est redevenue normale*. Retrieved from <https://www.rtbef.be/article/une-attaque-informatique-contre-l-universite-et-le-chu-de-liege-pendant-26-heures-la-situation-est-redevenue-normale-10999459>
- Portela, D., Nogueira-Leite, D., Almeida, R., & Cruz-Correia, R. (2023, June). Economic impact of a hospital cyberattack in a national health system: Descriptive case study. *JMIR Formative Research*, 7, e41738. doi: 10.2196/41738

- Rowe, B., & Gallaher, M. (2006). *Private sector cyber security investment strategies: An empirical analysis*.
- RTBF. (2021a, October). *Cyberattaque au chwapi: lent retour à la normale, certaines opérations encore postposées - rtbf actus*. Retrieved from <https://www.rtbf.be/article/cyberattaque-au-chwapi-lent-retour-a-la-normale-certaines-operations-encore-postposees-10677061>
- RTBF. (2021b, October). *Cyberattaque à la clinique saint-luc de bouge: un millier de consultations annulées ce lundi*. Retrieved from <https://www.rtbf.be/article/cyberattaque-a-la-clinique-saint-luc-de-bouge-un-millier-de-consultations-annulees-ce-lundi-10857609>
- RTL info. (2023, March). *“on a vite détecté une activité anormale”: le chu saint-pierre de bruxelles victime d’une cyberattaque*. Retrieved from <http://www.rtl.be/actu/belgique/faits-divers/vite-detecte-une-activite-anormale-le-chu-saint-pierre-de-bruxelles-victime-dune/2023-03-11/article/532226>
- Sente, A. (2022, May). *Attaque sur le réseau vivalia: les hôpitaux, cibles de choix des cybercriminels*. Retrieved from <https://www.lesoir.be/442643/article/2022-05-16/attaque-sur-le-reseau-vivalia-les-hopitaux-cibles-de-choix-des-cybercriminels>
- Sint-Andries Ziekenhuis. (2022, January). *Cyberaanval op sint-andriesziekenhuis*. Retrieved from <https://www.sintandriestielt.be/nieuws/cyberaanval-op-sint-andriesziekenhuis/>
- Smith, C. (2018). Cybersecurity implications in an interconnected healthcare system. *Frontiers of Health Services Management*, 35(1), 37–40. doi: 10.1097/HAP.0000000000000039
- van den Bosch, P., & Steenbruggen, W. (2024, July). *New draft cybersecurity act in the netherlands: What you need to know*. Retrieved from <https://biotalk.twobirds.com/post/102jexc/new-draft-cybersecurity-act-in-the-netherlands-what-you-need-to-know>
- Verdonck, J. (2022, January). *Ziekenhuis van tielt doelwit van cyberaanval*. Retrieved from <https://www.vrt.be/vrtnws/nl/2022/01/27/ziekenhuis-van-tielt-doelwit-van-cyberaanval/>
- Wilson, M. (2022, October). *Council post: Cyber insurance premiums are up—and that’s not the only industry shakeup*. Retrieved from <https://www.forbes.com/councils/forbestechcouncil/2022/10/21/cyber-insurance-premiums-are-up-and-thats-not-the-only-industry-shakeup/>
- World Health Organization. (2024, February). *Cyber-attacks on critical health infrastructure ga*. Retrieved from <https://www.who.int/news-room/questions-and-answers/item/cyber-attacks-on-critical-health-infrastructure>
- Yang, J. (2023, November). *Healthcare cybersecurity spending globally 2023*. Re-

trieved from <https://www.statista.com/statistics/1359081/cybersecurity-spending-in-healthcare-sector-worldwide/>

A Appendices

Figures

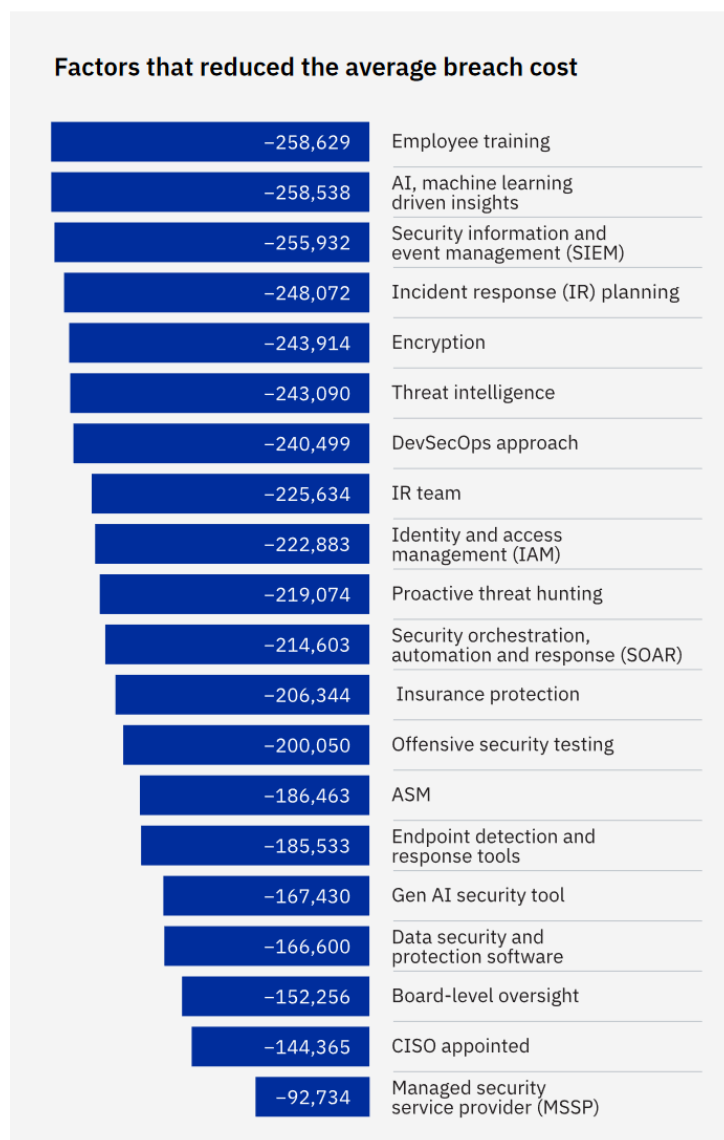


Figure 4: Cost difference from USD 4.88M breach average (IBM, 2024)

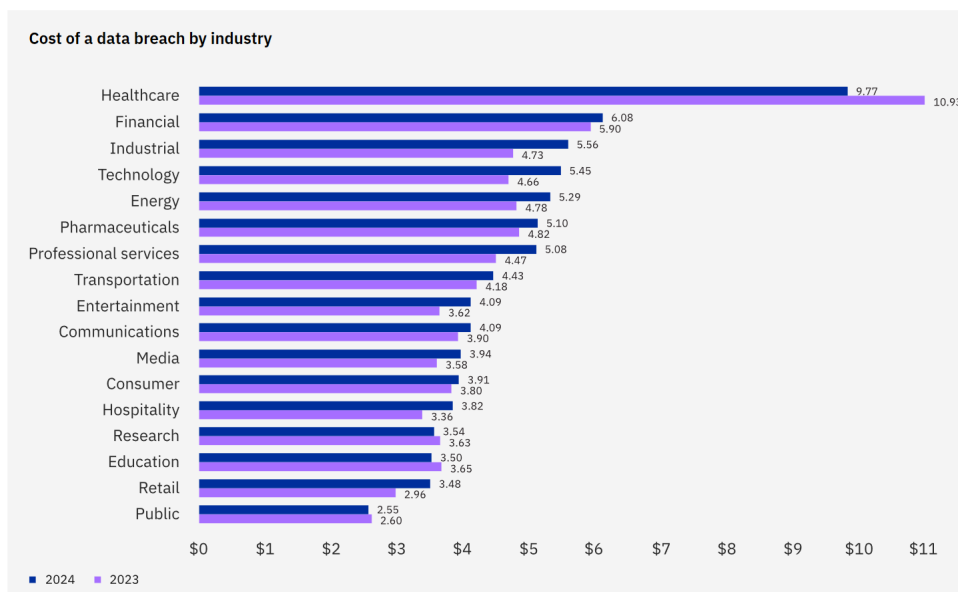


Figure 5: Cost of a data breach by industry, measured in USD millions (IBM, 2024)

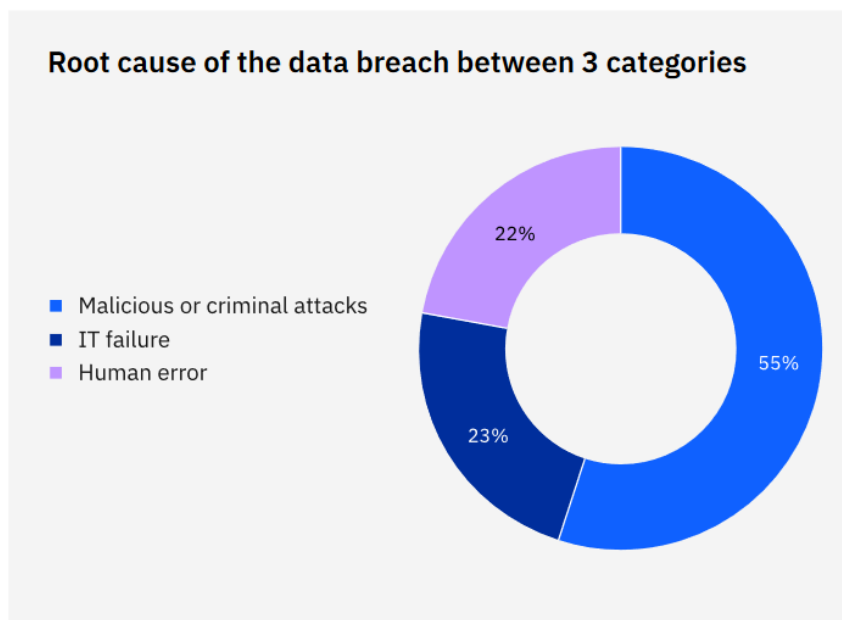


Figure 6: Cause of the databreach between 3 categories (IBM, 2024)

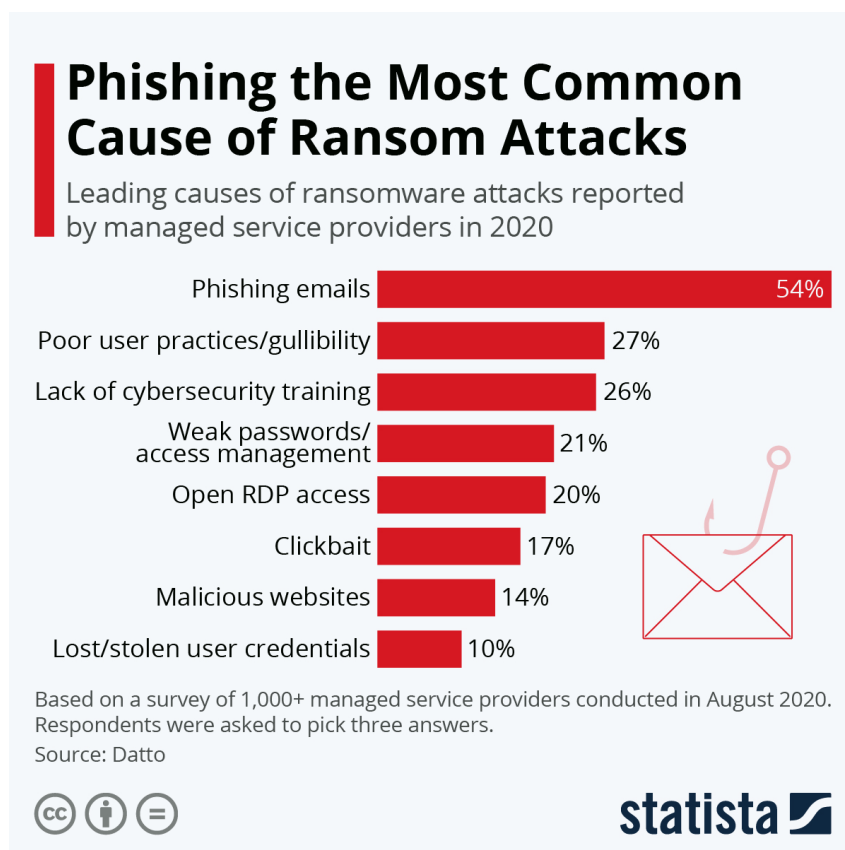


Figure 7: Causes of reported ransomware attacks in 2020. (Statista, 2020)

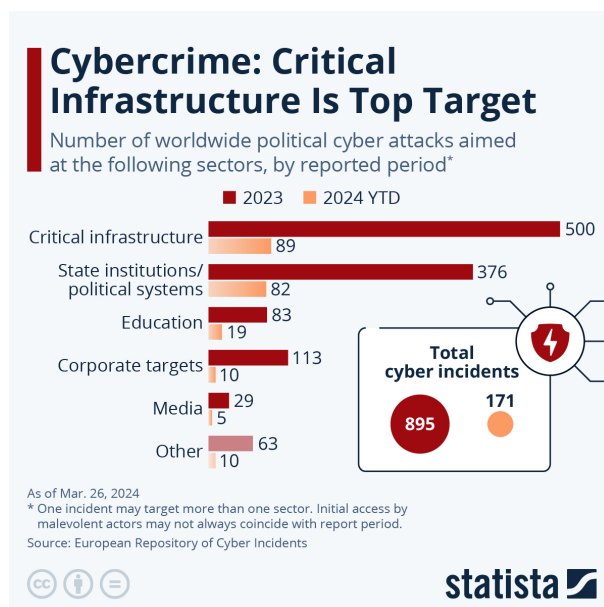


Figure 8: Number of worldwide cyberattacks aimed at critical infrastructure

Interviews

Retranscription of the interview with Pierre Colin, CIO of the Saint-Luc university hospital in Brussels:

Romain Ferrant: OK super merci beaucoup, donc voilà. Alors pour commencer les questions. Premièrement, est-ce que vous pourriez décrire brièvement votre rôle et vos responsabilités en tant que CIO à l'hôpital universitaire de Saint-Luc?

COLIN Pierre: En fait, je suis directeur en charge de l'informatique de l'hôpital. Donc j'ai une responsabilité globale, notamment sur la cybersécurité puisque j'ai dans mon équipe un CISO, hein, un Chief Information Security Officer. Voilà, j'ai la responsabilité opérationnelle, stratégique. C'est moi qui dirige le département informatique.

Romain Ferrant: OK et donc depuis combien de temps est-ce que vous occupez ce poste et est-ce que vous avez observé des changements notables dans le paysage de la cybersécurité pendant cette période ?

COLIN Pierre: Alors je suis ici depuis un an, mais par contre je suis pas nouveau dans la profession hein. Ça fait 30 ans que j'évolue dans la profession, mais avant ça, j'étais pas dans le secteur hospitalier. J'étais dans le secteur privé et dans le secteur des télécoms. J'ai travaillé pendant 30 ans pour des sociétés américaines et donc ça me donne une perspective très intéressante sur ce qui se passe ici, parce que c'est pas c'est pas du tout les standards auxquels j'étais habitué.

Romain Ferrant: OK et donc si on passe maintenant plus sur la stratégie de cybersécurité et le "Threat Landscape" comme on dit, quelles sont les principales menaces de cybersécurité auxquelles vous faites face quotidiennement à l'hôpital Saint-Luc ?

COLIN Pierre: Je veux dire que la menace la plus évidente ou la plus plausible. C'est le ransomware, hein, le rançon logiciel, et ça, ben on le sait.

COLIN Pierre: Parce que les hôpitaux sont des cibles de choix pour deux raisons. Un, parce que généralement, les hôpitaux sont moins bien protégés, d'un point de vue cybersécurité, que les banques ou les organismes gouvernementaux ou les entreprises commerciales, simplement parce qu'on a moins de moyens. Deuxièmement, les conséquences en cas d'attaque sont beaucoup plus directes puisque ça peut très très vite mettre des vies en danger.

Romain Ferrant: Oui en effet.

COLIN Pierre: Donc ça explique que pour certains cybercriminels, sans la moindre éthique, des hôpitaux représentent des cibles de choix, et je dis sans la moindre éthique parce qu'il se dit, hein, je sais pas si on a des statistiques sur les cybercriminels qui ne se laissent pas interviewer mais il se dit que certains cybercriminels n'attaquent pas les hôpitaux simplement parce qu'ils veulent garder une certaine éthique. Pourquoi attaquer un secteur qui est déjà en pénurie ? Et puis qui finalement, qui a un but sociétal ?

Romain Ferrant: Ouais, on va dire sûrement l'argent au final mais voilà. Vous avez donc dit que la menace la plus courante, c'est donc les ransomware. Et donc à quelle fréquence ? Enfin, ça fait qu'un an que vous êtes là, mais à quelle fréquence est-ce que vous gérez des incidents de ransomware et quels sont les points d'entrée habituels pour ces attaques ? Comment est-ce que ça commence ?

COLIN Pierre: Mais alors nous, Dieu merci, on n'a jamais eu affaire à du ransomware, donc je peux pas vous expliquer comment j'ai réagi dans le passé. On s'y prépare dans une certaine mesure, hein ? On n'est pas prêt, on est clairement pas prêt mais par contre on gère des alertes. On est régulièrement attaqué, en tout cas par des robots, hein, par des attaques de hameçonnage (phishing), des mails qui sont envoyés à notre personnel avec des liens malveillants, des virus. Des mots de passe qui sont subtilisés. Voilà, c'est on va dire que ce sont des attaques presque journalières, mais qui sont mineures. Et pour lesquelles on est bien protégé, donc elles ne portent jamais à conséquence mais c'est pratiquement journalier.

Romain Ferrant: OK, Oui et donc vous parliez du fait que vous ne pouvez pas vous protéger entièrement contre toutes les attaques. Mais quelles mesures spécifiques sont mises en place pour justement se protéger contre ce type d'attaque et potentiellement les ransomware ?

COLIN Pierre: En fait, la cybersécurité, ça repose sur plusieurs piliers. Y a d'abord très certainement la détection. C'est-à-dire savoir qu'on est attaqué, savoir que quelqu'un s'est introduit, c'est important. Donc on travaille sur cet axe-là, j'y reviendrai. Après, comment est-ce qu'on fait ? Il y a certainement être prêt à répondre en cas d'attaque, ça veut dire ça. C'est vraiment un très gros travail pour savoir. Bon, ce sont des plans de contingences, ce sont des plans de mise en quarantaine et donc y a plusieurs techniques pour ça. Il y a la restauration du service, donc une fois qu'on a répondu à l'attaque, qu'on a éventuellement jugulé l'attaque, Bah quelles sont les démarches à suivre pour restaurer le service, euh. Et donc on travaille surtout sur ces piliers. Là, y a la sensibilisation, la formation du personnel. Et donc c'est vraiment un gros programme. La cybersécurité,

on travaille sur sur sur beaucoup de piliers. Je peux éventuellement vous présenter, euh, une slide. Elle résume assez bien les différentes initiatives.

Romain Ferrant: Voilà donc là, on a un peu parcouru manière globale, mais donc le secteur de santé santé en particulier, est très visé, comme vous le disiez car voilà il y a enfin par rapport aux institutions privées ou gouvernementales, peut-être y a-t-il moins de budget d'une part et à part ça, est-ce qu'il y a d'autres vulnérabilités qui rendent enfin y a aussi le fait que ce sont des données très critiques qui sont traitées et donc est-ce qu'il y a des vulnérabilités spécifiques qui rendent les hôpitaux et les institutions très attrayantes pour les cybercriminels.

COLIN Pierre: Évidemment hein, donc on a parlé du manque de moyen. C'est un secteur qui n'a pas, ne dispose pas des mêmes moyens financiers pour mettre en place un programme de cybersécurité et l'activer rapidement. Il y a les conséquences directes, mais il y a aussi la difficulté à sécuriser l'environnement. Une banque, c'est assez facile à sécuriser, on ferme les portes, on met des barreaux sur les fenêtres. Un hôpital, c'est un hall de gare, on doit accepter tout le monde dans un hôpital et je vais dire, on doit même aller plus loin, on doit accepter même les criminels dans un hôpital. Donc un hôpital est ouvert au public, par définition. Euh donc c'est extrêmement difficile à sécuriser d'un point de vue périmètre. Puisque c'est une institution qui est ouverte au public et donc ça, c'est tout à fait particulier au secteur hospitalier.

Romain Ferrant: Et est-ce que au niveau technologique que ce que le fait que les hôpitaux sont non dépendant de beaucoup de systèmes informatiques qui sont peut-être dus, justement à un manque de budget pas toujours au top de la, enfin à la pointe de la technologie, est-ce que c'est aussi une raison que les hôpitaux sont plus visés ?

COLIN Pierre: Alors, il y a deux points, il y a le fait que les soins de santé de manière générale sont de plus en plus dépendants de la technologie, donc ce qu'il faut imaginer c'est que aujourd'hui on prend une salle d'opération, le médecin, il a plusieurs écrans devant lui, dont le dossier patient, il a accès aux imageries, par exemple de radiographie ou scanner. Il a accès à tout l'historique du patient, il peut éventuellement les consulter. Le jour où l'informatique ne fonctionne plus, ça devient très compliqué de garantir la continuité des soins dans un hôpital, que ce soit en salle d'opération, aux urgences, au laboratoire et donc la dépendance à la technologie et à l'informatique est devenue très très critique. Et ça, c'est nouveau parce qu'il y a 15 ans, c'était pas le cas ou en tout cas pas dans la même mesure.

COLIN Pierre: Aujourd'hui, le laboratoire, donc le laboratoire, c'est extrêmement important dans un hôpital puisque si vous venez aux urgences ou un patient est admis aux urgences, première chose qu'on va faire, c'est une prise de sang. Prendre des paramètres

des analyses qui doivent partir au laboratoire et les résultats doivent revenir rapidement. Souvent, si c'est pour une urgence, hein, c'est savoir que le laboratoire, il est largement robotisé, on a des robots, donc des automates, puis vont effectuer.

C'est plus un humain qui analyse les analyses sanguines, et cetera. Ça fait par des robots, ces robots sont pilotés par l'informatique. Si l'informatique n'est plus disponible, ben là on doit retomber sur un mode manuel, mais c'est beaucoup plus lent, donc il y a tout un impact. Idem par exemple, pour l'imagerie ou la pharmacie, la pharmacie est hautement robotisée, donc, pour avoir accès à un médicament ou un implant ou une prothèse dont on a besoin durant l'opération ? Ben l'informatique doit être fonctionnelle, sinon ça devient beaucoup plus compliqué, donc il y a une très très grosse dépendance à la technologie qui ne fait que croître et ça c'est une donnée dont on doit tenir compte.

Alors l'autre, l'autre aspect, c'est qu'on a d'excellentes technologies, donc on a des technologies de pointe à l'hôpital, mais ça ne veut pas dire pour autant qu'elles sont sécurisées. Vous imaginez qu'un et ça représente aussi une des difficultés spécifiques au monde hospitalier, c'est que c'est un environnement informatique qui est extrêmement hétérogène. Ça veut dire qu'on a sur notre réseau un nombre d'équipements incalculables que nous ne contrôlons pas. Pourquoi ? Bah par exemple, un scanner en radiographie pour être utilisable, il doit être accordé à un serveur à des PC et souvent c'est une firme externe. La firme, par exemple Philips ou bien Sony qui est le fabricant qui va venir installer toute cette solution qui est connectée sur notre réseau, et on n'a pas trop le choix à cette solution nous est imposée et si on devait effectuer des tests de pénétration sur cet environnement, peut-être que c'est pas le plus sécurisé du monde, mais nous on a aucun contrôle dessus et l'hôpital est absolument rempli de ce type d'équipement, ils peuvent représenter des voies d'entrée, donc on a des technologies de pointe, mais elles sont pas toujours sécurisées.

Et la complexité ou le coût pour les sécuriser, de maintenir appropriée, est très lourd parce que l'évidence, c'est la segmentation des réseaux, hein, qui va bientôt nous être imposée par la norme NIS2. Mais c'est extrêmement lourd. Moi, si je dois segmenter le réseau de la manière dont on voudrait le faire pour le sécuriser de manière adéquate pour un hôpital, je pense que je dois engager deux personnes en plus. Et je peux pas engager deux personnes en plus, donc voilà, c'est un petit peu les challenges auxquels on fait face.

Romain Ferrant: Et donc, concrètement, que visent les cybercriminels avec un ransomware dans un hôpital ? Parce que c'est comme vous disiez, c'était les ransomware le plus gros danger, qui prennent en otage les données, les encryptent et demandent une rançon de façon monétaire. Est-ce que ce qu'ils visent alors plus des données patients,

ou est-ce qu'ils bloquent justement certains réseaux informatiques ou l'utilisation de machines ?

COLIN Pierre: En fait. Les cybercriminels, et qui vont utiliser du ransomware hein du rançon logiciel. Leur objectif, c'est d'extirper de l'argent.

COLIN Pierre: D'accord, donc qu'est-ce qu'ils vont utiliser comme technique ? Ils vont essayer de rendre l'hôpital inopérant, donc de casser un maximum ou de rendre inopérationnel un maximum de système pour nous pousser à payer une rançon. Mais généralement, on connaît et ça a été le cas, par exemple, la dernière grosse attaque dans le monde hospitalier en Belgique, c'était à Namur, hein ? Au CHSM, à Namur.

J'ai été les rencontrer donc je sais très bien ce qui s'est passé. Euh, et ça se passe toujours en deux étapes, c'est à dire que avant d'encrypter les données ils vont essayer de les voler, donc de les exfiltrer. Évidemment, ils se gardent bien de le dire. Généralement, ils demandent une première rançon. Parce que là, ils ont mis le système à l'arrêt puisqu'ils ont tout encrypté donc tout s'arrête. Et dans le cas où on paierait la rançon ou même si on ne paye pas la rançon mais qu'on arrive à restaurer le système, parce qu'on avait des sauvegardes qui ont été sécurisées hein ? Parce que généralement, ce qu'ils font, c'est qu'ils détruisent d'abord les sauvegardes, ou ils les encryptent.

Et puis ils encryptent la production, ce qui fait qu'on ne sait plus utiliser les sauvegardes pour restaurer le service. Mais même alors il y a pas mal de technologies qui permettent de se prémunir de ça. Mais au cas où on arriverait à restaurer le service sans payer la rançon, généralement un mois ou deux plus tard, ils vont venir avec une deuxième demande de rançon en montrant qu'ils ont des données en leur possession et en menaçant de placer ces données à la vente sur le Dark Web, des choses comme ça. Donc c'est connu, c'est que l'on paye la rançon pour éventuellement décrypter les systèmes qui ont été encryptés, ou qu'on ne la paye pas, ils viendront de toute manière par après en une deuxième étape avec une demande de deuxième rançon s'ils sont parvenus à exfiltrer des données.

Romain Ferrant: Et enfin, quel impact est-ce que ça a sur la sécurité des patients et la confidentialité de leurs données ?

COLIN Pierre: Quelle est l'impact ? Si les systèmes sont à l'arrêt. Ça pourrait mettre en danger certains patients. Euh, c'est un petit peu difficile. Bien que les médecins et l'hôpital soient relativement préparés pour faire face à une panne d'informatique limitée dans le temps, Si, imaginons on a des chirurgiens qui sont en pleine opération et que les systèmes informatiques s'arrêtent, ils peuvent terminer leur opération ou peut-être ne pas

l'effectuer, ou s'arrêter là où ils sont. Un médecin est formé pour faire face à ce genre de situation, donc a priori on ne devrait pas mettre en danger la vie des patients, mais voilà, il y a quand même un risque, hein, qui n'est pas nul de mettre la vie en danger, mais après l'impact, bah l'impact c'est : L'impossibilité de soigner les patients correctement, On devrait fermer l'hôpital, rediriger les urgences vers d'autres hôpitaux. Donc l'impact, c'est très solide.

Romain Ferrant: OK, et d'un point de vue financier donc, heureusement, vous n'avez pas encore été victime de ransomware, mais de manière générale, que pensez-vous qu'il serait l'impact financier d'une attaque sur un hôpital que ce soit l'impact direct et puis indirect dû à la récupération des données par exemple, ou des amendes ou pénalités ?

COLIN Pierre: Ça peut être colossal, ça peut être colossal, potentiellement. Ça pourrait amener l'hôpital à la faillite. L'hôpital, il a des charges qu'il doit payer, et des remboursements des emprunts, des factures à payer, et s'ils ne soignent plus il n'y a plus d'argent qui rentre. Et ça peut aller très très vite, hein ? Parce que avec le ransomware, on peut faire face à des interruptions de plusieurs semaines avant qu'on puisse restaurer le service. Alors, l'hôpital pourrait parer aux urgences uniquement, c'est-à-dire imaginons un scénario catastrophe avec toute l'informatique à l'arrêt. On devrait fermer l'hôpital, ne garder que les patients qui sont intransportables, mais on devrait renvoyer beaucoup de patients chez eux ou vers d'autres hôpitaux. C'est ce qui s'est passé à Namur d'ailleurs hein ? Donc au niveau impact financier, c'est colossal ça, c'est direct. Et puis, en indirect, y a toute la gestion de crise. C'est sûr que si on avait une attaque, on va très très rapidement (et on a des contrats en place pour ça) faire appel à des sociétés extérieures pour venir nous aider, mon personnel informatique n'est pas le plus performant pour faire face à une attaque, donc directement on va avoir des coûts parce qu'on va demander de l'aide externe pour venir nous aider.

Romain Ferrant: Et est-ce que d'un point de vue légal il y a des implications aussi si par exemple des données patients enfuies ?

COLIN Pierre: Bah oui, oui, il y a des implications légales, on a l'obligation par la loi de répondre à certaines normes en matière de sécurité et notamment on s'attend, comme la norme NIS2 en Belgique. C'est une norme qui a été votée au niveau de la Commission européenne. Ça, c'est dans les lois, on doit répondre à certains standards. Maintenant, quel serait le risque couru par l'institution si les données de certains patients devaient être subtilisées, ça, moi, je suis pas expert pour pouvoir chiffrer le préjudice. Mais certains patients pourraient naturellement poursuivre l'hôpital. Alors il faudra préétablir des responsabilités et voir si l'hôpital a manqué à ses devoirs en matière de protection cybersécurité.

Romain Ferrant: Et donc de manière générale, alors, quelles sont les mesures proactives que vous mettez en place pour prévenir justement les attaques ?

COLIN Pierre: Donc on a d'abord l'accent sur la protection, c'est à dire qu'on essaie de fermer les fenêtres et les portes, hein, donc là où on sait qu'on a des vulnérabilités. On a mis à jour, on a remplacé nos pare-feux, par exemple, à des pare-feux beaucoup plus intelligents. Euh, on utilise une nouvelle technologie réseau. Enfin, et c'est on a encore énormément de vulnérabilités auxquelles on doit remédier, mais c'est vraiment un très long processus, simplement parce qu'il y a tout un changement de mentalité.

COLIN Pierre: On parle beaucoup, on parle beaucoup de 0 trust, hein. C'est en matière de cyber risk, cybersécurité, qu'est-ce que ça veut dire ? Ça veut dire que auparavant, je veux dire jusqu'il y a peut-être 15 ans, on considérait qu'il fallait bien fermer les portes et les fenêtres. Mais une fois qu'on était à l'intérieur de la maison, ou du réseau, en l'occurrence, on était sécurisé. Et maintenant c'est fini, on travaille plus du tout comme ça, on a ce concept de 0 trust qui veut dire qu'on est en sécurité nulle part, même à l'intérieur du réseau.

Donc, typiquement auparavant, quand on développait des applications internes elles étaient accessibles à travers un navigateur, par un site web. Ben on jugeait pas utile d'encrypter la communication si ça restait à l'intérieur du réseau puisque on se considérait en sécurité à l'intérieur du réseau. Maintenant, c'est plus du tout comme ça quand on déploie des applications web, même si elles ne sont accessibles qu'à l'intérieur du réseau, on encrypte le trafic, voilà, ça a un des exemples les plus parlants. Mais ça veut dire que par exemple, quand on accède au VPN, donc on veut se connecter au réseau à distance. On considère qu'à distance, on n'est pas sécurisé, donc on va demander un double facteur pour l'authentifier passe plus encore. Alors que en 0 trust, on va dire qu'on soit à l'extérieur ou à l'intérieur, on demande toujours un double facteur par exemple, donc voilà le concept de 0 trust, ça veut dire qu'on fait confiance à personne où que l'on soit.

Et donc il faut le même niveau de sécurité qu'on soit à l'extérieur qu'à l'intérieur du réseau. Ça, ça implique de repenser complètement l'architecture des systèmes informatiques parce qu'ils étaient pas pensés pour ça, donc on ne sait pas passer de l'ancien système au nouveau sur une année ou deux, c'est vraiment un travail de longue haleine et ça, c'est surtout donc sur le pilier protection, donc ça veut dire qu'il y a des vieux serveurs qui ont des vulnérabilités à remplacer par des nouveaux.

COLIN Pierre: Mais souvent, ces vieux serveurs sont là pour une raison, parce qu'ils hébergent une application qu'on a achetée il y a bien longtemps et dont on a toujours

besoin. Mais le vendeur a disparu, donc elle n'est pas compatible avec la dernière version de Windows ou de Linux. Donc on est obligé de garder ce vieux serveur qui est bourré de vulnérabilités. Alors, quelle est la solution ? Là par exemple, ben on place le serveur sur un segment du réseau complètement isolé. Comme ça, si jamais ce serveur est exploité, de là où il est, on ne peut aller nulle part. Bah tout ça, ça demande énormément de ressources, hein.

Donc voilà, c'est vraiment au niveau de la protection, le type d'initiative que l'on déploie.

Ensuite, ce qu'on fait, ce sont des tests de pénétration. On demandera avec des sociétés externes, ce qu'on appelle les « Red Team », hein, ce sont les méchants ici. Ils vont faire du hacking éthique, c'est-à-dire qu'ils vont rien casser, mais ils vont essayer d'identifier quelles sont les vulnérabilités qu'il y a chez nous.

On a aussi des outils qui nous identifient les vulnérabilités. Euh, au niveau de la détection, ben là c'est un des plus gros projets qu'on a menés récemment. Cette année, on a déployé un SOC, un Security Operation Center, avec un SIEM qui est un Security Information and Event Management. Euh, c'est quoi ? C'est une application, on va dire, c'est un Data Lake qui collecte des informations de type sécurité de tous nos systèmes critiques, donc par exemple, les pare-feux, Active Directory, les Antivirus, les ODR, tout ça qui est centralisé.

Il y a des algorithmes de corrélation pour détecter des événements anormaux au niveau de la sécurité. Donc ça, c'est robotisé et alerte le Security Operation Center, qui est une firme avec laquelle on a enfin qu'on a contracté, avec laquelle on a un contrat et qui elle est opérationnelle 24h sur 24. Parce que moi je n'ai pas une équipe assez grande pour pouvoir travailler 24h sur 24 et donc ça, on externalise. On a déployé un SOC donc qui nous permet à priori de savoir si quelqu'un est chez nous, ou s'il y a une intrusion, y a quelque chose d'anormal, donc là c'est une autre initiative.

COLIN Pierre: D'accord donc voilà en gros donc au niveau détection au niveau réaction, là c'est pour plus tard. Cette année, on prépare la mise au point de plans de redémarrage. On fait aussi des exercices de simulation avec le métier. On travaille avec les salles d'opération, avec les urgences, avec le laboratoire, la radiographie. On leur dit, tiens, si là maintenant il n'y avait plus d'informatique. Comment réagiriez-vous ? Comment pourriez-vous traiter ce patient ? Des exercices aussi, hein, pour être prêt en cas de réelle attaque.

Et puis au niveau de la récupération, on travaille beaucoup sur la sécurisation des sauvegardes puisque si jamais on devait être attaqué, on sait que la cible numéro un des criminels, c'est d'abord les sauvegardes. Parce que s'ils encryptent nos serveurs et qu'on sait qu'on peut les réparer facilement parce qu'on a des sauvegardes qui sont fiables et inattaquables, ben déjà on va pas payer la rançon. L'idée c'est d'être prêts en cas d'attaque parce qu'on sait très bien que le risque zéro n'existe pas. Il y aura toujours une possibilité d'être attaqué, donc il faut être prêt à être attaqué. Voilà en quelques mots comment on travaille sur la cybersécurité.

Romain Ferrant: Et en termes de formation et sensibilisation du personnel à travers l'hôpital entier, comment faites-vous ? C'est vous qui gérez ça aussi, ou pour ça, vous faites appel à des sociétés externes ? Mais comment éduquez-vous et formez-vous le personnel sur les risques de cybersécurité et les best practices ?

COLIN Pierre: Alors là c'est aussi quelque chose qu'on a fait dans les six derniers mois. On a fait l'acquisition d'un outil qui fait ça tout seul, en gros, donc c'est un outil intégré qui envoie des faux messages, c'est-à-dire, ce sont des mails de phishing. Sauf que les liens ne sont pas malveillants, mais les liens nous permettent de détecter le personnel qui se laisse prendre dans les filets, hein, et on suit avec les personnes qui sont faits attraper pour que, à leur tour, elles suivent des formations qui font partie du même outil. L'outil lui-même offre les formations et nous permet à nous de suivre qui a suivi la formation ou pas. Donc on a des tableaux de bord qui nous permettent de voir notre progrès en matière de sensibilisation du personnel, c'est important.

Le risque principal est humain, c'est avant tout, les gens qui ne sont pas vigilants avec leur mot de passe ou qui vont cliquer sur un lien malveillant. Les grands risques sont de ce côté-là.

Romain Ferrant: Et donc grâce à cette application, ça permet d'assurer donc que tous les membres du personnel adhèrent au protocole de cybersécurité ?

COLIN Pierre: Ça permet donc aux personnels de se former pour pouvoir reconnaître soit des mails, des messages malveillants et poursuivre les bonnes pratiques, hein, d'utiliser des mots de passe complexes, ne pas divulguer son mot de passe, ne pas utiliser le même mot de passe que sur notre système. Enfin voilà, c'est-à-dire à former le personnel à avoir une bonne conduite en matière de cybersécurité.

Romain Ferrant: OK voilà. Alors que moi je suis arrivé un peu, on a un peu abordé la plupart de ce que je voulais aborder et donc si maintenant j'aimerais bien passer sur

une partie de perspective future, donc sur les menaces émergentes par exemple. Est-ce qu'il y a des grands défis auxquels vous faites face actuellement ou qui vont émerger ? Pour maintenir une cybersécurité robuste avec par exemple l'avancée des IA et cetera récemment ?

COLIN Pierre: Alors ce qu'on lit, hein ? Dans les études, c'est que, euh, évidemment, l'avènement de l'intelligence artificielle est également exploité par les cybercriminels pour affiner leur technique et les rendre encore plus efficaces. Euh donc ça je pense que c'est une menace réelle, mais je dirais que d'une manière plus macro, le problème est qu'on se bat contre un ennemi qui est beaucoup plus fort que nous puisque le marché de la cybercriminalité, ça fait longtemps qu'il rapporte plus d'argent que le marché de la drogue ou des stupéfiants et c'est un business donc extrêmement lucratif. Et donc les cybercriminels disposent de moyens colossaux. Euh, et donc c'est là qu'est la difficulté, y compris l'accès aux technologies comme l'intelligence artificielle. Et donc ça, ça présente un réel défi. Mais donc je veux dire tant que le monde en général n'est pas mieux organisé pour traquer et punir les cybercriminels, je vois mal comment on va aller inverser la tendance, donc c'est clair que l'intelligence artificielle représente un outil fantastique, y compris pour des fins malveillantes.

Romain Ferrant: Et quelles sont donc alors les menaces les plus grandes ? Qui, enfin, les menaces de cybersécurité émergentes ou enfin déjà existantes ? Mais qui vous préoccupent le plus ?

COLIN Pierre: Euh ben pour le moment, c'est carrément le ransomware parce qu'on sait que c'est ce qui affecte le plus largement le secteur hospitalier, mais on commence à parler et ce sont des études qui le montrent, on commence à parler de wipeware et de killware, je sais pas si vous avez déjà entendu parler de ça. Donc là le but du ransomware, c'est d'extirper de l'argent à travers une rançon. Le wipeware, c'est juste de détruire. Alors, quel est l'objectif de détruire ? Éventuellement dans un but de déstabilisation d'un État, puisque on sait qu'on a des pays qui sponsorisent ou qui financent des groupes de cybercriminels à des fins géopolitiques. Et donc on pourrait très bien imaginer la Russie ou la Chine qui inventent un plan de détruire tous les hôpitaux en Belgique ou en France.

Pas pour de l'argent mais pour déstabiliser le pays, donc ça c'est du wipeware, mais je pense que c'est seulement émergent ou anecdotique pour le moment, mais on s'en méfie. Et alors le killware, bien, comme le nom l'indique, le killware, c'est donc attaquer les services, enfin des solutions technologiques informatiques avec l'objectif de tuer quelqu'un, une personne en particulier ou plusieurs, c'est un business, peut être beaucoup plus efficace et moins risqué que d'engager un Albanais pour aller tuer l'amant de sa femme.

Voilà, on pourrait imaginer que et là, ça, ça représente un danger réel, surtout dans les hôpitaux. Imaginez que quelqu'un qui a l'intention de vous tuer. Par exemple, il sait que vous devez venir subir une transfusion dans un hôpital ou une opération, si il arrive à s'introduire dans les systèmes et échanger votre groupe sanguin dans votre dossier, l'affaire est faite... Et ça, ça fait peur parce que là on ne parle plus d'argent, mais on parle de la vie des gens. Je pense pas que ce soit quelque chose d'extrêmement répandu comme du Ransomware et là moi j'ai pas de chiffres, mais on m'a averti que ça pouvait représenter un risque. Pour le moment, on ne le considère pas très au sérieux et surtout que en fait, la manière de se prémunir du killware, du wipeware ou du ransomware ce sont les mêmes mécanismes, donc ça ne change rien à notre stratégie.

Romain Ferrant: OK, donc alors pour finir, quelles améliorations/changements est-ce que vous aimeriez voir dans l'infrastructure de cybersécurité de votre hôpital ?

COLIN Pierre: Je pense que c'est essentiellement du financement. On parle beaucoup des financements des soins de santé en Belgique ou en Wallonie, qui est un réel problème. Le problème numéro un, c'est de financer l'opérationnel, donc les infirmiers, les médecins, et déjà rien que ça c'est un problème. Mais il faudrait mettre l'accélérateur pour l'informatique et la cybersécurité, ça c'est le changement que tout le monde demande. Parce que moi, avec mon bagage, je viens du privé, donc j'ai connu des niveaux de protection bien supérieurs et une maturité dans la cybersécurité. Donc ça m'aide énormément dans la sécurisation de l'hôpital. Mais on avance bien trop lentement à mon goût, uniquement par manque de moyens. Et donc ce qui pourrait changer les choses, c'est qu'on dispose de plus de moyens.

Romain Ferrant: Tout retombe au final sur des moyens financiers. Enfin, le manque de moyens financiers dans le secteur hospitalier. Est-ce que vous pensez que c'est particulier à la Belgique et est-ce que, par exemple, la privatisation des hôpitaux changerait quelque chose à cela ?

COLIN Pierre: Alors je ne sais pas répondre à cette question parce que j'ai pas une vue globale sur le secteur de la santé, que ce soit en Belgique ou en comparaison avec d'autres pays. Donc ça, j'ai pas d'avis. Ce que je sais, c'est que par exemple dans les hôpitaux américains, qui, eux, sont privatisés, effectivement ils sont plus avancés, donc ça pourrait être une des réponses. Sauf que privatiser les hôpitaux, c'est complètement repenser le système belge, donc je pense qu'on n'y est pas.