Ransomware Attacks on the UK National Health Service (NHS) and Ireland Health Service Executive (HSE): Case Studies and Defense Strategies

ABSTRACT

Background

Ransomware attacks in Healthcare Organizations have become a tool of disruption for Malicious actors with the intent of crippling healthcare activities, compromising patient treatments and data in return for financial gain. In the last decade, the NHS and HSE have faced serious challenges in managing and mitigating ransomware incidents which have exposed critical weaknesses in both organizations' cybersecurity preparedness, incident response, and recovery strategies.

Objectives

This thesis was aimed at evaluating the existing Ransomware incident response strategies employed by the NHS and HSE between 2017 and 2024, identify gaps and design a comprehensive and practical Incident Response Plan using the PICERL framework based on the realities of the healthcare organizations.

Results

Findings indicate that the NHS and HSE lack effective, centralized leadership and clearly defined cybersecurity IR roles, while recovery and proactive threat detection measures remain underdeveloped. Both organizations struggled with implementing standards like ISO 27001 and integrating advanced tools like CTI and SIEM into their response strategies.

Findings

The proposed strategy incorporates preparation, continuous monitoring, and AI tools that emphasize affordability and practicality. Recommendations focus on structured communication, enhanced recovery systems, and continuous threat detection to safeguard healthcare organizations.

Keywords: Ransomware, Incident Response, PICERL, NHS, HSE.

INTRODUCTION

Background of The Study and Research Problem

Ransomware attacks in the UK and Ireland national Healthcare sectors—NHS and HSE—have become a menace in recent times leading to consequences of cyber threats that extend beyond technical vulnerabilities. O'Kane, Sezer, and Carlin (2018) describe Ransomware as a malware that renders a victim's computer or data unusable. It is a malicious software threat designed by Cyber criminals to lock system users out of a system network and deny access to the system or data until a stipulated ransom is paid (O'Kane, Sezer, and Carlin 2018). Ransomware attacks have become increasingly popular and sophisticated in recent years, causing the fear of data loss faced by most organisations when under attacks (O'Gorman and McDonald 2012). In the UK, the National Health Service (NHS) has experienced widespread disruptions due to ransomware attacks. Similarly, Ireland's Health Service Executive (HSE) has been faced with severe Ransomware attacks leading to serious negative impact on patient care and public health services (Kaberuka and Johnson 2023). According to Minnaar and Herbig (2021), the targeting of the healthcare sector, which for several reasons has become more vulnerable to cyberattacks than most other sectors has ultimately led to the endangerment of not only the lives and health of patients, but has also put nurses, doctors and other healthcare workers at even greater risk. Ransomware attacks have negatively impacted the treatment protocols and delayed the provision of essential services, such as medical operations, leading to the overall disruption of the provision of medical and healthcare services in Ireland and the UK (Minnaar and Herbig 2021).

Several cyber security experts have attributed the popularity of ransomware attacks to the healthcare institutions increasingly digitizing their operations and relying on interconnected technologies, which has unfortunately, made them become more attractive targets for ransomware attacks (Thamer and Alubady 2021). Kaberuka and Johnson (2023) emphasize that vulnerabilities in healthcare systems are most of the time caused by poor technical maintenance of network systems, ignorance of cyber vulnerabilities,poorly protected cyber infrastructure and impractical response plans.

Problem Significance and Motivation

The extent of the popularity of recent ransomware attacks in the NHS and HSE has led to certain risk liabilities and negative impacts associated with such attacks (Spence, Bhardwaj

and Paul III 2018). Ransomware attacks on healthcare systems are more than just technical breaches; they threaten patient safety, disrupt essential services, and generate enormous financial and reputational losses (Neprash et al. 2022). However, unfortunately, for healthcare organizations like the NHS and HSE, which operate on tight budgets and serve millions of patients, such attacks can cause severe operational and financial damage. This study will offer insights for Cyber security experts, Researchers and Stakeholders into the security gaps in the existing incident response plans used by these organizations and explore how improved defense strategies can mitigate risks.

Research Question and Objectives

The research question for this thesis is: "*How can the NHS and HSE effectively defend against and mitigate the impact of ransomware attacks using a comprehensive Incident Response Plan?*"

Objectives

- To investigate the evolution of Ransomware and its impacts on the NHS and HSE
- To critically evaluate the NHS and HSE cyber security strengths against ransomware attacks using the PICERL framework
- To critically evaluate the recent NHS and HSE Ransomware attacks, examining the types of malware used, techniques employed, vulnerabilities exploited and recovery plans using the PICERL framework.
- To evaluate the effectiveness of the current NHS and HSE Ransomware incident response plans
- Design a Ransomware Incident response plan for the NHS and HSE to strengthen their resilience against future ransomware attacks.

Limitations and Scope

The limitations of this research is embedded in its research methodology and scope. The research would analyse Ransomware Attacks targeted to the NHS and HSE from 2017- 2024. All resources for analysis would be dated from 2017-2024 to provide a recent scope of research and evaluation.

Research Methodology

The study will adopt a qualitative research approach, relying on secondary data through a comprehensive literature review. Academic articles, government reports, incident analyses, and cybersecurity frameworks will be explored to understand the nature of ransomware attacks

and defense mechanisms. Case studies of the NHS and HSE attacks will also be analyzed to identify patterns, vulnerabilities, and responses using the PICERL framework to develop an incident response plan.

Structure of the Thesis

1. Introduction: introduce the topic of ransomware attacks on the NHS and HSE, outline the research problem, motivations, research questions, objectives, limitations and scope.

2. Literature Review: indepth review of existing literature on ransomware, including historical perspectives, related literature on cybersecurity defense strategies for the NHS and HSE and gaps in the previous studies.

3. Methodology: outline the methodologies employed for data sourcing and collection, research design, case study analysis, and framework used for the research design.

4. Case Studies Analysis and Discussions: provide detailed descriptions of NHS and HSE ransomware incidents,vulnerabilities exploited, common patterns of attacks, and the defensive measures taken and discuss them to identify gaps in current defense strategies.

5. Conclusion and Recommendations: summarise the key findings of the research and recommend a detailed incident response plan for the NHS and HSE healthcare infrastructures to prepare, contain and recover from Ransomware attacks.

LITERATURE REVIEW

2.1 Overview of Ransomware and Cyber Threats: Historical Perspectives and Current Perspectives

It is interesting to note that ransomware as sophisticated as it is today, did not begin as such. The origin of Ransomware can be traced back to the year 1989, when the first Ransomware malware, PC Cyborg, was developed by Joseph L. Popp (Seth et al. 2022). Popp became popular after hacking the conference of AIDS by WHO causing 18000 files to become infected and encrypted with the PC Cyborg, and demanded payment for a decryption tool (Richardson and North 2017). However, the encryption was weak, allowing cybersecurity experts to eventually develop tools to recover the data.

Since then, The PC Cyborg has laid the foundation for modern ransomware by demonstrating the potential of holding digital assets hostage(Richardson and North 2017). Following the failure of the first Ransomware attack, in 1996, Adam L. Young and Moti Yung introduced

more advanced prototypes (Gorman and McDonald 2012). This was followed by the advent of cryptographic ransomware, such as Cryptolocker which was created by Slavik in 2013, which encrypted files with strong algorithms, making recovery impossible without the decryption key (Saiyed 2016).

Now, Ransomware attacks have further evolved by incorporating new delivery methods, such as phishing emails, malicious advertisements, and drive-by downloads. These improvements have been accompanied by a move towards as-a-service models (Ransomware-as-a-Service), where criminals can purchase ransomware kits to carry out attacks without technical expertise (Ryan 2021; O'Kane, Sezer and Carlin 2018). This shift has lowered entry barriers and increased the frequency of attacks (Greenstein 2022). This Ransomware model has increased the access to sophisticated malware, allowing a wide range of attackers to target individuals, corporations, and public institutions by lowering the barriers to entry for cybercrime (Singh et al. 2024; Keijzer 2020; Alwashali, Rahman and Ismail 2021).

Following the lucrativeness of Ransomware attacks, attackers have switched their targets from individual users to organizations and big companies with the aim of demanding huge ransoms (Khan and Ansari 2019), which has been aided by the invention of Bitcoin by Satoshi Nakamoto for safe decrypted money transfers. According to Ahn, Doupe, Zhao and Liao (2016), most Ransomware attacks became successful due to the attacker's ability to block access to a computer system or data by encrypting it, facilitating the attacker to demand payment in cryptocurrencies, such as Bitcoin.
These developments have transformed ransomware from a basic malware into a highly organized cybercrime tool, posing significant risks to critical infrastructure and public safety.

2.2 Ransomware Threat in the NHS and HSE: Cybersecurity Challenges and Impact of Ransomware

The healthcare sector has become particularly vulnerable due to its reliance on interconnected IT infrastructure (Pattnaik et al. 2023). Pattnaik et al. (2023) further that organizations most attractive for ransomware attacks typically share certain characteristics: they rely heavily on digital infrastructure, hold valuable or sensitive data, and face significant operational consequences if their systems are taken offline. Healthcare providers, for instance, are frequent targets due to the critical nature of their work. Delays in treatment or access to medical records

can have fatal consequences, making hospitals more likely to pay ransoms quickly (Minnaar and Herbig 2021).

According to Moore et al. (2021), for the NHS and HSE, Ransomware attacks can result in the cancellation of surgeries, delays in treatment, or even patient deaths when critical systems fail. Additionally, the theft and release of sensitive data can damage reputation, erode patient trust, and lead to regulatory penalties under data protection laws such as the General Data Protection Regulation (GDPR). Financially, the cost of a ransomware attack extends beyond the ransom itself, encompassing costs related to incident response, system restoration, legal fees, and lost revenue during downtime (Moore et al. 2021).
Porcedda (2023) states that the attacks on the NHS in 2017 and HSE in 2021 exemplify the potential for operational paralysis when cybersecurity fails. Beyond immediate disruptions, the impact of these attacks were profound. At an operational level, the Ransomware attacks led to halt medical functions, delay essential services, and significant financial losses (Porcedda 2023).

According to Harvey et al. (2023), The NHS and HSE ransomware incidents provided insight into how attacks unfold and how healthcare organizations respond. In both cases, attackers exploited vulnerabilities in system configuration and software patches. While the NHS attack highlighted weaknesses in legacy systems, the HSE incident emphasized the risks posed by delayed responses to cyber warnings (Coventry et al. 2020). According to Coventry et al. (2020), these cases showed that recovery strategies in both organizations varied based on institutional preparedness, availability of backups, and external partnerships.

On another level, Stritch, Winterburn and Houghton (2021) argue that the attacks were made possible due to the several cybersecurity infrastructural challenges facing both the NHS and HSE, including outdated infrastructure, insufficient investment in IT security, and staff lacking cybersecurity awareness. Zarocostas (2021) also explains that these Healthcare systems are pressured to maintain availability and confidentiality while managing high patient loads, often resulting in suboptimal cyber hygiene.

Furthermore, Minnaar and Herbig (2021) posit that the COVID-19 pandemic exacerbated these challenges, as healthcare institutions scrambled to manage increased cyberattacks while prioritizing patient care. Also, Bryce, Khatib and Vinny (2023), add that the shift toward

telehealth introduced vulnerabilities in remote monitoring tools and communication channels, increasing windows for Ransomware attacks.

2.4 Review of Related Literature: NHS and HSE Ransomware Causes, Defense Strategies, Prevention and Mitigation

The study by Kaberuka and Johnson (2023) emphasized a socio-technical approach to analyzing ransomware incidents, focusing specifically on the WannaCry attack on the UK's NHS and the cybersecurity attack on the Irish healthcare system, their study revealed that Ransomware attacks are often a product of both technical vulnerabilities and operational deficiencies, which over time degrade working practices. Similarly, Al-Qarni (2023) in his review of cyberattacks on healthcare institutions, attributed their high susceptibility to outdated security protocols and limited resources dedicated to cybersecurity. He argued that hospitals and healthcare providers are prime ransomware targets due to the high sensitivity and value of patient data. To mitigate ransomware in healthcare, Al-Qarni emphasized that robust security measures, including encryption, regular system updates, employee training in cybersecurity awareness, clear data recovery protocols and real-time monitoring of network activity are essential.

Additionally, Harvey et al. (2023) explored the specific impact of a Ransomware attack on HSE and effects on disrupted patient care. He suggests that to mitigate the effects of such attacks on clinical trials, emphasis on the importance of "cyber maturity," particularly within healthcare, should be encouraged. This can include regular cyber assessments, incorporating cyber incident response plans across all participating institutions, and establishing clear communication channels to facilitate quicker recovery. According to Harvey et al (2023) a successful mitigation solution should include both organizational preparedness and technological defenses.

In another note, Porcedda (2021) in her analysis of HSE) ransomware attacks points to limitations in the regulatory frameworks such as the National Cyber Security Centre and the Data Protection Commission and suggests they be provided with more operational capacity to increase their effectiveness in preventing and responding to large-scale attacks.

2.5 Review on the Efficiency of Current NHS and HSE Cybersecurity Incident Response Plans: DSPT and ICT FRAMEWORK

In light of the repetitive Ransomware attacks on the NHS and HSE, there have been implementations of incident response plans and policies aimed at catering to these cyber security threats faced by both organizations. However, in spite of this, the problem of Ransomware attacks still persists. Some scholars like Kaberuka and Johnson (2023), Coventry et al. (2020) and Harvey et al. (2023) have associated the continuous attacks to ineffectiveness and lack of practicality of the incident response plans based on the socioeconomic structure of these healthcare organizations.

Another study by He et al. (2022) showed the limitations of most cyber incident response (IR) strategies by highlighting that these IR procedures, commonly employed by organizations like the NHS and HSE, are predominantly reactive, being designed to respond to attacks after they occur, leaving healthcare systems vulnerable to emerging threats.

As implied by these scholars, the effectiveness of these incident response plans proposed to these organizations have continued to provide limited solutions to the persistent problem of Ransomware attacks. Mashinchi, Acton and Datta (2024) highlights the gaps in proactive cybersecurity and recovery strategies embedded in the HSE, cyber security response plan—ICT Framework. In their analysis of the HSE ICT Framework, they identified significant shortcomings in its ability to prevent and mitigate ransomware attacks. The study showed the HSE's overreliance on reactive measures rather than proactive cybersecurity strategies, which has exacerbated the impact of Ransomware attacks the organization has experienced, especially the Conti Ransomware attack of 2021 (Mashinchi, Acton and Datta 2024). Furthermore, Mashinchi, Acton and Datta (2024) explain that the ICT Framework, while outlining measures for addressing cyber threats, fails to prioritize early detection and threat-hunting capabilities. This gap has left the HSE vulnerable to sophisticated attacks that exploit systemic weaknesses such as outdated systems, and insufficient risk management practices. The authors argue that the HSE's framework relies mostly on recovery from cyber incidents rather than employing preemptive measures to identify and neutralize cyber threats before they manifest.

Similarly, the findings from Kaberuka and Johnson (2023) study emphasized the socio-technical complexities of healthcare cybersecurity. They argued that frameworks like the ICT Framework must incorporate comprehensive risk assessments that address both technical and human factors (Kaberuka and Johnson 2023).

For the NHS response plan—The DSP Toolkit (DSPT), cyber security scholars have highlighted the shortcomings of the strategy. For one, Tully et al. (2020) in their study on the NHS WannaCry 2017 attack, demonstrated how despite the DSPT's focus on compliance and reporting, lacked the robust mechanisms needed to proactively combat sophisticated ransomware attacks. Tully et al. (2020) argued that while existing disaster preparedness plans like the NHS's DSPT incorporate "all-hazards" frameworks, these are insufficient for the unique challenges posed by cyberattacks. While the DSPT emphasizes governance, staff awareness, compliance, reporting and reactive incident management, it does not fully integrate advanced threat intelligence or predictive analytics to foresee and prevent attacks. Also, it falls short in terms of recovery preparedness and has no detailed recovery plan for post-incident scenarios especially when compared to IR plans like NIST Cybersecurity Framework (Tully et al. 2020).

2.6 Gaps in the Literature

Many literature on ransomware's impact on healthcare systems, specifically the NHS and HSE, often highlight the need for technical and policy defenses to combat cyberattacks. However, while these recommendations offer valuable insights, they frequently overlook the sector-specific challenges that healthcare organizations face. Although Incident Response Plans by the NHS and HSE like DSPT and ICT Framework respectively, have sought to answer to the problem of Ransomware attacks, they have also proven short in addressing the issue. Based on the studies reviewed in the literature, critical gaps and limitations of the NHS and HSE incident response strategies remain include a lack of emphasis on proactive recovery preparedness, lack of real-time Cyber Threat monitoring and insufficient alignment of incident response plans (IRPs) with the socioeconomic constraints and operational complexities of these organizations.

Using the PICERL framework (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned), this thesis will propose innovative incident response strategies that incorporate real time ransomware monitoring, recovery preparedness and innovation cybersecurity trends while putting into consideration the socioeconomic structure realities of the NHS and HSE while enhancing security. The proposed response plan wiill not only address current shortcomings but also lay the foundation for a forward-looking, and further development in achieving resilient cybersecurity posture, ensuring patient safety and operational continuity.

METHODOLOGY

This study employed a literature review based research approach and the PICERL Framework to explore Ransomware attacks on the UK NHS and Ireland HSE. It was employed to conduct the study's literature review and real-world Ransomware case study reviews while the PICERL framework was employed in order to provide defense strategies and an incident response plan for ransomware tailored to the suit the healthcare infrastructure of the NHS and HSE based on the nature and impact of the Ransomware attacks both organizations had experienced.

3.1 The Data Collection Methods

The data collection method for this study was purely a literature review based methodology. A literature review can broadly be described as a more or less systematic way of collecting and synthesizing previous research (Synder 2019; Tranfield, Denyer, and Smart 2003).

In this study, the literature-based methodology involved using various forms of literature to gather data, providing comprehensive insights into ransomware and cybersecurity incidents. Data was collected from academic journals and articles, Peer-reviewed journals to gather foundational theories, historical contexts, and trends in ransomware, NHS and HSE organizational and industry reports, including cybersecurity incident response reports, and operational responses used during the NHS and HSE Ransomware attacks.

Data Collection Sources

This study utilized various data collection sources such as digital academic libraries, academic publications platforms, including Google Scholar, Academia, ResearchGate, ACM library, JSTOR, Journal of Statistics Education, NHS and HSE publications.

3.2 Ethical Considerations

Using a literature review based research approach often presents some ethical considerations, oftentimes involving concerns about accuracy and research quality (Arifin 2023; Steffen, Lyons and Coyle 2016). Hence, this study made sure to abide by the essential ethical guidelines and procedures throughout the research process. The data collected was secured from only trusted academic sources, and open source digital publications to avoid ethical and copyright

issues. In addition, all resources were obtained in line with NCI declaration of ethics consideration guidelines to ensure that research met the institution's ethical standards.

3.3 Research Design and Data Analysis

The PICERL framework fm was used for the case study analysis. The PICERL framework involves Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned which guides the framework in providing and recommendation of cyber security incident response strategies. The data analysis included the six stages of PICERL:

- **Preparation:** involved assessing pre-attack cybersecurity readiness within the NHS and HSE, including policies, training, and technology used to prevent ransomware.
- **Identification:** reviewed how each organization detected and identified ransomware threats
- **Containment:** explored immediate actions taken to limit the spread of ransomware
- **Eradication:** examined methods used to remove ransomware and neutralize threats, focusing on the technical solutions and protocols followed.
- **Recovery:** focused on steps taken to restore critical systems and data, assessing how each organization regained full operational functionality.
- **Lessons Learned:** analyzed post-attack evaluations, organizational changes, and recommendations to improve future resilience and risk mitigation.

3.4 Justification of the Chosen Methodological Approach and Framework

A literature review-based methodology was chosen for this study due to a variety of carefully thought out reasons. Firstly, it allowed for a comprehensive analysis of ransomware attacks in healthcare by synthesizing data from various scholarly sources, incident reports, and technical papers (Synder 2019). This approach was suitable because it leveraged documented cases, industry publications, and academic research to study both NHS and HSE attacks, providing an in-depth understanding. Secondly, using existing literature also facilitated a broad, systematic comparison of healthcare cybersecurity strategies and responses across different case studies, which enabled this study to identify strengths, weaknesses, and impacts of defense strategies that were applicable to other healthcare organizations.

The PICERL framework was chosen for structuring the analysis because it covered the full lifecycle of a cybersecurity incident. This framework was well-suited for evaluating defense strategies, breaking down each phase of the ransomware response process, facilitating a clear, organized comparison of the NHS and HSE's responses and outcomes.

CASE STUDY ANALYSIS AND DISCUSSION

4.1 Overview of Ransomware Attacks in the NHS and HSE

4.1.1 WannaCry Attack on the NHS (2017)

On May 12, 2017, there were reports of a large Wannacry Ransomware attack global which affected the NHS. This cyber attack exposed some of the cyber security weaknesses of the NHS (Dwyer 2018). Following the incident, several Trusta and primary care services across England and Scotland were severely impacted for many days after the initial entry of the malware into the networks. Although the NHS was not a direct target as it was a victim of a global cyber incident that affected over 230,000 computers in 150 countries caused by vulnerabilities in Microsoft Windows called EternalBlue (Ghafur et al. 2019). Most of the NHS devices that were infected with the ransomware, were found to have been running an unpatched Microsoft Windows 7 OS which was the cause of the Ransomware spread (Matin et al. 2018). In addition, the ransomware spread was also traced to the N3 network which was the broadband network connecting all NHS sites in England (Ghafur et al. 2019).

The attackers used the Eternalblue vulnerability to exploit the Microsoft Server Message Block 1.0 of the Windows 7 OS which is a file sharing protocol that allows applications on a computer to read and write to files and to request services on the same network (Prevezianou 2021). Also, reports of the attack analysis revealed links to the Lazarus group who had been linked to North Korea (Wheeler and Alderdice 2022).

4.1.2 Immediate and long-term Impacts of the Attack on the NHS

The 2017 WannaCry attack has been referred to as the largest Ransomware attack in history (O'Dowd 2017). Key NHS systems were blocked, preventing staff from accessing patient data and delivery of critical services such as outpatient appointment, hospital emergencies, radiology, pathology, surgical procedures and elective admissions (Aljaidi et al. 2022). The incident was reported to have left a total of 81 out of 236 hospital Trusts and 595 out of 7,545 general practices affected and an estimated 1,000 equipments which resulted in the cancellation of about 20,000 appointments (O'Dowd 2017).

The long-term impact of the incident, according to Mahmoud (2024) included Financial losses which reported cost the NHS close to £92million, disruptions in NHS operations, reputational damage resulting from failure to protect sensitive data, Loss of trust from patient, impact on

the economy, legal consequences and the highlighting of systemic vulnerabilities in IT infrastructure.

4.1.3 Incident Response: How the NHS Handled the Incident

The NHS collaborated with the National Cyber Security Centre (NCSC) to contain the spread of the malware (Johnson 2018). The NHS issues by providing guidelines that outlined strategies to contain the Ransomware including disconnection of affected systems from networks while recovery teams worked towards restoring systems and reinstalling software patches on compromised devices (Johnson 2018).

According to Ghafur et al. (2019), since the incident, the UK government has raised funds towards the upgrade of systems and improvement of cybersecurity capabilities across the NHS.

4.1.4 Lessons Learned: Shortcomings in Preparation and Response

The NHS (2017) report identified several shortcomings in IR preparation and recovery and lessons learned from the WannaCry attack including, how underinvestment and low budgets in cybersecurity combined with lack of accountability resulted in an overall weak security posture and the need for sufficient investment in cybersecurity, failure to install update patches on network despite the issuance of warnings months prior to the attack, lack of properly structured incident response plan, lack of recovery system backups, lack of sophisticated IT systems, lack of staff training on cyber attack handling and cyber security, and delay in incident reporting and handling (Wirth 2018; NHS 2017).

4.1.5 Conti Ransomware Attack on the HSE (2021)

In May 2021, the Irish public health service (HSE), was the target of an aggressive Ransomware cyber-attack that affected and paralysed almost the entire state healthcare sector (Stritch, Winterburn and Houghton 2021). The Conti Ransomware attackers demanded a Ransom of $20 million which the HSE refused to pay, leading to over a month of its systems not operational (Harvey et al. 2022). According to Moore et al. (2023), the Conti Ransomware was initiated through a phishing email that allowed attackers to infiltrate the system. The response by the HSE resulted in the widespread removal of access to ICT systems as Hospital staff were forced to revert to pen and paper (Moore et al. 2023).

4.1.6 Impact of the Attack Across HSE Operations

According to Stritch, Winterburn and Houghton (2021), it took four months to completely recover from the attack, with HSE sustaining numerous impacts to healthcare delivery during this timeframe. The Conti Ransomware attack left the HSE with severe negative impacts including, the shutdown to healthcare services putting patient care and safety at risk, the inaccessibility of patients records on the HSE system, financial loss, loss of integrity and public confidence (Stritch, Winterburn and Houghton 2021). The attack triggered a Critical Incident Process, followed by the shutdown of all HSE IT systems in the country which led to disruptions to patient care across the HSE's 4000 locations, 54 acute hospitals, and 70,000 connected devices (Harvey et al. 2022). Additionally, the attack cost the HSE estimated €100 million for repairing and upgrading the Irish health system's IT infrastructure.
Other impacts of the attack included legal consequences from patients lawsuits over interrupted patient treatments, patient data theft, and data breach (Harvey et al. 2022).

4.1.7 Incident Response: Analysis of the HSE's Incident Response

The attack left the HSE confused and disoriented on how to proceed with an Incident Response Plan as no hospital cyberattack emergency plan was in place (Keogh et al. 2024). The HSE sought collaboration from external and international cyber security agencies, including the NCSC and private cybersecurity firms, to investigate and contain the attack (Keogh et al. 2024). The recovery plan included IT systems shutdown and recovering data from unaffected systems (Keogh et al. 2024).

4.1.8 Lessons Learned: Challenges in Recovery and Mitigation.

The Conti Ransomware attack on the HSE exposed gaps in HSE's cybersecurity approach. Reports showed that the HSE lacked comprehensive cyber incident response leadership at senior executive or management level at the time of the incident (Mashinchi, Acton and Datta 2024). Also, the lessons learned from the incident included in the HSE 2021 report post incident review showed the need to implement a comprehensive leadership governance structure in the, HSE and National Health Network (NHN) over IT and cybersecurity to provide appropriate focus, attention and oversight, need to provide a well-documented, use of Modernized IT system, tested incident response plan, and increase cybersecurity awareness and preparedness at all organizational levels (HSE 2021; Mashinchi, Acton and Datta 2024).

4.2 Discussion: Comparative Analysis of NHS and HSE Incident Response Plans

4.2.1 DSP Toolkit (NHS) vs ICT Framework (HSE)

As aforementioned in the literature review, the Incident Response Plans of the NHS and HSE possess critical weaknesses including lack of effective leadership and communication protocols, overreliance on responsive measures rather than preparatory, proactive measures for threat detection and prevention (Mashinchi, Acton and Datta 2024; He et al. 2022), lack of well documented IR strategies for Ransomware attacks, insufficient provision for cyber security awareness and training on IR guidelines (Kaberuka and Johnson 2023; Coventry et al. 2020).

4.2.2 Assessment of Responses and Handling of Ransomware Incidents in NHS and HSE

The analysis of the Ransomware incident response strategies of the NHS and HSE revealed some systemic weaknesses and key themes in cyber security government, incident response planning, preparedness and recovery capabilities.

4.2.2.1 Lack of Clearly Defined Responsibilities and Security Preparedness

It can be seen from the incident responses that due to NHS' and HSE complex structures, there was a lack of clearly defined responsibilities and security preparedness in the face of a cyberattack which exacerbated the attacks and contributed to limited resilience in both organizations respectively. The HSE lacked an effective centralized cybersecurity function overseeing risk management and mitigation. This lack of proper leadership and defined structure in the HSE delayed their ability to provide a response strategy that would have facilitated quick incident responses effectively. Instead, the absence of a dedicated IR leadership threatened the cyber security posture of the HSE and exacerbated the Ransomware spread.

Similarly, the NHS' IR showed gaps in preparedness, as most of the network consisted of outdated IT systems, leaving the organization vulnerable, leading to the WannaCry attack. Despite the availability of the Data Security and Protection Toolkit (DSPT) at the time of the attack, due to its lack of practical implementation and financial constraints, the NHS was ill-equipped to follow through on the stipulated IR.

4.2.2.2 Lack of Tested Incident Response Planning

At the time of the incident, both the HSE and NHS lacked rigorously tested IR plans. In the case of the HSE, the Conti ransomware attack exposed that their IR planning was primarily reactive and had not been sufficiently tested under realistic conditions. This lack of preparation resulted in the shutting down of the national HSE system, disrupting over 50 hospitals and diagnostic delays.

The NHS, on the other hand, though equipped with the DSPT framework, also struggled with inadequately tested response mechanisms. The aftermath of the WannaCry attack revealed that many NHS Trusts did not have robust contingency plans or drills to mitigate the impact of such an event. The limited understanding of the implementation of IR and the lack of comprehensive testing caused the NHS response to be delayed and heavily reliant on external agencies like the UK NCSC.

4.2.2.3 Inadequate Implementation of ISO 27001 Practices

Neither organization fully adhered to ISO 27001 standard for managing information security. In the HSE's case, this failure to implement robust risk assessment and management practices made the organization a prime target for the Conti ransomware attack. Also, the lack of centralized oversight and failure to address weaknesses in cybersecurity controls, such as outdated software and insufficient network segmentation led to inconsistent application of security controls.

The NHS exhibited similar shortcomings. While policies aligned with ISO 27001 existed on paper, their application was hindered by resource limitations, limited adherence, implementation and incomprehensive risk assessment frameworks and audits resulting in persistence of key vulnerabilities in NHS systems, leaving the organization exposed to ransomware threats.

4.2.2.5 Limited Recovery Preparedness

Both organizations demonstrated a strong lack of recovery preparedness that prolonged downtime and exacerbated the financial and reputational damage caused by ransomware incidents. The HSE's recovery process, for instance, relied heavily on external and international cybersecurity agencies, revealing the absence of an internal recovery strategy. Similarly, the NHS struggled to restore operations during WannaCry, as outdated systems and inadequate recovery protocols delayed efforts.

4.3 Recommendation

As highlighted by the discussions, the IR employed by the NHS and HSE lacked adequate accountability. Hence addressing these issues requires a framework that enables concerted

effort to promote and instill comprehensive understanding of Ransomware preparedness and responsive measures.

4.3.1 Proposed Ransomware Incident Response Plan for the NHS and HSE

This proposed Incident Response Plan adopts the PICERL Framework (Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned), which builds on the current NHS DSPT 2024-2025 toolkit and the HSE ICT Framework by addressing specific gaps and shortcomings while introducing new measures that are cost-effective to enhance cybersecurity resilience to suit the needs of the resource-constrained realities of both healthcare organizations.

Preparation Phase

- **Training and Simulations**
    - Conduct routine cybersecurity training and workshops for staff at all levels to understand the importance of cybersecurity education and to recognize threats such as phishing attempts.
    - Implement real-world attack simulations to test the organization's preparedness and response efficiency.
- **Effective IR Leadership and Structure**
    - Establish a dedicated IR Team with clearly defined roles and responsibilities, including senior leadership oversight.
    - Assign a Chief IR Team Leader to oversee the strategy and execution of IR.
    - Develop a governance framework that integrates cybersecurity oversight into organizational IR and National Health Network (NHN) decision-making processes.

- **Structured Communication Protocols**
    - Create predefined communication protocols to ensure clear, timely, and consistent information flow during an incident.
    - Set up secure communication channels for internal and external stakeholders, patients, and regulatory bodies.

    - Designate spokesperson(s) to manage public relations and minimize misinformation during an incident.
- **ISO 27001 Implementation and Integration**
    - Fully adopt ISO 27001 practices to create a centralized and systematic approach to cybersecurity risk management.
    - Perform regular audits and updates to maintain compliance.
- **Collaboration For Shared Resources and Partnerships**
    - Collaborate with national cybersecurity agencies like the NCSC for the NHS and CSIRT for the HSE to enhance threat intelligence sharing.
- **Risk Assessment and Continuous Monitoring**
    - Conduct comprehensive evaluations of vulnerabilities and threats. This can be achieved using affordable tools such as open-source risk assessment frameworks, CIS Controls Assessment Tool and Security Information and Event Management (SIEM) tools for threat hunting and addressing key weaknesses proactively.
- **Recovery Backup Systems**
    - Perform backups daily frequently
    - Maintain offline backups disconnected from the network to protect against ransomware infiltration
    - Use Cloud-based backups solutions to provide scalability and redundancy.

Identification

- A**dvanced CTI Tools**
    - Integrate Cyber Threat Intelligence (CTI) tools like SIEM to monitor, collect, and analyze threat data.
    - Use Endpoint Detection and Response (EDR) for endpoint-level insights to detect extent of attack.

Containment

- **Network Segmentation**
    - Immediately segment networks to isolate critical systems to reduce Ransomware

- **Access Control**
    - Implement strict user authentication policies including MFA or zero-trust architectures.

Eradication

- **AI-Driven Threat Removal**
    - Use AI-based threat detection tools to automatically identify and remove malicious software.
    - Deploy EDR solutions to eliminate ransomware traces.

Recovery

- **Tailored Recovery Plans**
    - Implement chosen backup solutions to quickly restore systems
- **Proper Documentation**
    - Documentation of IR actions and decisions for future reference.

Lessons Learned

- C**ontinuous Improvement Cycles**
    - Conduct post-incident reviews and audits to evaluate response effectiveness and update plans for future response protocols.

This IRP is recommended for both the NHS and HSE to significantly improve their cybersecurity posture, ensure business continuity, and resilience in the ransomware attacks.

EVALUATION AND CONCLUSION

5.1 Evaluation

The objectives of this thesis were to assess the strength and weaknesses of the current NHS and HSE Ransomware IRPs to pinpoint their weaknesses and gaps in order to recommend

stronger IR measures. To address this objective, this thesis has thoroughly explored the background to the study, problem statement, literature review which detailed the evolution of Ransomware, impact of Ransomware attacks in the NHS and HSE, and gaps in the incident responses of both organizations. It has also designed and recommended a comprehensive Ransomware IRP for the NHS and HSE with consideration of the limited funding situation of both organizations.

5.2 Summary of Analysis and Discussions

The comparative analysis of the NHS and HSE response to ransomware incidents pointed toward series of gaps and shortcomings in their IRP, including cybersecurity governance, lack of cyber threat preparedness, ineffective responses, lack of defined leadership, roles and responsibilities, and limited recovery capabilities in the Ransomware IR plans of both organizations.

Conclusion

This thesis provides a comprehensive solution to the failures in the Ransomware IRP of the NHS and HSE by its proposed tailored incident response strategy using the PICERL framework to address highlighted gaps, while ensuring affordability and practicality. It contributes to the academic field by bridging gaps in healthcare cybersecurity, by introducing a cost-effective, scalable incident response framework, with detailed competent proactive measures. The findings will guide future research in safeguarding critical healthcare infrastructures against evolving Ransomware threats.

BIBLIOGRAPHY

Ahn, G.-J., Doupe, A., Zhao, Z. & Liao, K., 2016. Ransomware and cryptocurrency: Partners in crime. In *Cybercrime Through an Interdisciplinary Lens*, pp.119-140.

Aljaidi, M., Alsarhan, A., Samara, G., Alazaidah, R., Almatarneh, S., Khalid, M., & Al-Gumaei, Y.A., 2022. NHS WannaCry ransomware attack: technical explanation of the vulnerability, exploitation, and countermeasures. 2022 International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI), pp.1-6.

Al-Qarni, E.A., 2023. Cybersecurity in healthcare: A review of recent attacks and mitigation strategies. *International Journal of Advanced Computer Science and Applications*, 14(5).

Ali Alwashali, A.A.M., Rahman, N.A.A. & Ismail, N., 2021. A survey of ransomware as a service (RaaS) and methods to mitigate the attack. *2021 14th International Conference on Developments in eSystems Engineering (DeSE)*, pp.92-96.

Arifin, S.R.M., 2018. Ethical considerations in qualitative study. *International Journal of Care Scholars*, 1(2), pp.30–33.

Bryce, C., El Khatib, R. & Vinny, A., 2023. Implications of telemedicine in care homes: Considerations for the evolving risk landscape. Lockton LLP.

Coventry, L., Branley-Bell, D., Sillence, E., Magalini, S., Mari, P., Magkanaraki, A. & Anastasopoulou, K., 2020. Cyber-risk in healthcare: Exploring facilitators and barriers to secure behaviour. International Conference on Human-Computer Interaction, pp.105-122.

Datta, P.M. & Acton, T., 2023. From disruption to ransomware: Lessons from hackers. Journal of Information Technology Teaching Cases, 13(2), pp.182-192.

Dwyer, A. 2018. The NHS cyber-attack: A look at the complex environmental conditions of WannaCry. RAD Magazine, 44(512), pp.25-26.

Collier, R., 2017. NHS ransomware attack spreads worldwide. *CMAJ*, 189(22), pp.E786-E787.

Ghafur, S., Grass, E., Jennings, N.R., & Darzi, A., 2019. The challenges of cybersecurity in health care: the UK National Health Service as a case study. *The Lancet Digital Health*, 1(1), pp.e10-e12.

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P., 2019. A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ Digital Medicine*, 2(1), p.98.

Greenstein, B., 2022. The impact of ransomware-as-a-service on critical infrastructure. Utica University.

Harvey, H., Amberger-Murphy, V., Ballot, J., O'Grady, M., O'Hare, D., Lawler, G., Bennette, E., Connolly, M., McNevin, C., Noone, E., Kelly, M.G., Bazin, A., Kearns, K., Mulroe, E., McDermott, R.S., & O'Reilly, S., 2022. Impact of Conti ransomware attack on cancer trials Ireland sites. *Journal of Clinical Oncology*, 40(16_suppl), pp.e13614-e13614.

He, Y., Maglaras, L., Aliyu, A. & Luo, C., 2022. "Healthcare Security Incident Response Strategy-A Proactive Incident Response (IR) Procedure." Security and Communication Networks (1), 2775249.

HSE, 2021. Conti cyber attack on the HSE - Independent Post Incident Review. PWC. Available at: https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf [Accessed 5 December 2024].

Johnson, K., 2018. National Resilience in CyberSpace: The UK's National Cyber Security Strategy Evolving Response to Dynamic Cyber Security Challenges. *Univerzita Karlova, Fakulta sociálních věd*.

Kaberuka, J. & Johnson, C., 2023. Case studies in the socio-technical analysis of cybersecurity incidents: Comparing attacks on the UK NHS and Irish healthcare systems. Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media: Cyber Science 2022, pp.375-387.

Keijzer, N., 2020. The new generation of ransomware: An in-depth study of Ransomware-as-a-Service. University of Twente.

Keogh, R.J., Harvey, H., Brady, C., Hassett, E., Costelloe, S.J., O'Sullivan, M.J., Twomey, M., O'Leary, M.J., Cahill, M.R., O'Riordan, A., Joyce, C.M., Moloney, G., Flavin, A., Bambury, R.M., Murray, D., Bennett, K., Mullooly, M., & O'Reilly, S., 2024. Dealing with digital paralysis: Surviving a cyberattack in a National Cancer center. Journal of Cancer Policy, 39, p.100466.

Khalid, O., Ullah, S., Ahmad, T., Saeed, S., Alabbad, D.A., Aslam, M., Buriro, A. & Ahmad, R., 2023. An insight into machine-learning-based fileless malware detection. Sensors, 23(2), p.612.

Khan, N.A. & Ansari, M.T.J., 2019. Ransomware: A digital extortion. Language, 6(4).

Mahmoud, K., 2024. WannaCry Impact And How Adoption Of Cyber Crime Measures Such As ISO 27001 Can Be Beneficial. 04/06/2024, pp.1-11.

Mashinchi, M.I., Acton, T. & Datta, P.M., 2024. "When healthcare becomes sick: Recovering from ransomware." Journal of Information Technology Teaching Cases, 0(0), .1–10.

Mattei, T.A., 2017. Privacy, confidentiality, and security of health care information: Lessons from the recent WannaCry cyberattack. *World Neurosurgery*, 104, pp.972-974.

Martin, G., Ghafur, S., Kinross, J., Hankin, C., & Darzi, A., 2018. WannaCry—a year on. *BMJ*, 361.

Meland, P.H., Bayoumy, Y.F.F. & Sindre, G., 2020. The Ransomware-as-a-Service economy within the darknet. Computers & Security, 92, p.101762.

Minnaar, A. & Herbig, F.J.W., 2021. Cyberattacks and the cybercrime threat of ransomware to hospitals and healthcare services during the COVID-19 pandemic. Acta Criminologica: African Journal of Criminology & Victimology, 34(3), pp.155-185.

Moore, G., Khurshid, Z., McDonnell, T., Rogers, L. & Healy, O., 2023. A resilient workforce: Patient safety and the workforce response to a cyber-attack on the ICT systems of the national health service in Ireland. BMC Health Services Research, 23(1), p.1112.

Moran Stritch, M., Winterburn, M., & Houghton, F., 2021. The Conti ransomware attack on healthcare in Ireland: Exploring the impacts of a cybersecurity breach from a nursing perspective. Canadian Journal of Nursing Informatics, 16(3-4).

Mundt, M. & Baier, H., 2023. Threat-based simulation of data exfiltration toward mitigating multiple ransomware extortions. Digital Threats: Research and Practice, 4(4), pp.1-23.

Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system.

Neprash, H.T., McGlave, C.C., Cross, D.A., Virnig, B.A., Puskarich, M.A., Huling, J.D., Rozenshtein, A.Z. & Nikpay, S.S., 2022. Trends in ransomware attacks on US hospitals, clinics, and other healthcare delivery organizations, 2016-2021. JAMA Health Forum, 3(12), p.e224873.

NHS, 2018. NHS England Lessons Learned Review of the WannaCry Ransomware Cyber Attack. Available at: https://www.england.nhs.uk/wp-content/uploads/2018/02/06_pb_08_02_18-lessons-learned-review-wannacry-ransomware-cyber-attack.pdf [Accessed 5 December 2024].

O'Dowd, A., 2017. Government must "get its act together" over cyberattacks on NHS, says watchdog. BMJ, 359.

O'Gorman, G. & McDonald, G., 2012. Ransomware: A growing menace. Symantec Corporation.

O'Kane, P., Sezer, S. & Carlin, D., 2018. Evolution of ransomware. IET Networks, 7(5), pp.321-327.

Pattnaik, N., Nurse, J.R.C., Turner, S., Mott, G., MacColl, J., Huesch, P. & Sullivan, J., 2023. It's more than just money: The real-world harms from ransomware attacks. International Symposium on Human Aspects of Information Security and Assurance, pp.261-274.

Porcedda, M.G., 2023. The ransomware attack against the Irish Health Service Executive: What role for the law in the face of growing cyber insecurity? Irish Jurist (N.S.), 70, p.322.

Prevezianou, M.F., 2021. WannaCry as a creeping crisis. In Understanding the Creeping Crisis, pp.37-50.

Richardson, R. & North, M., 2017. Ransomware: Evolution, mitigation, and prevention. 13(1), p.1021.

Saiyed, C., 2016. CryptoLocker. ISSA Journal, 14(4).

Seth, R., Sharaff, A., Chatterjee, J.M. & Jhanjhi, N.Z., 2022. Ransomware Attack: Threats & Different Detection Techniques. In Information Security Handbook, pp.157-176.

Spence, N., Bhardwaj, M.B. & Paul III, D.P., 2018. Ransomware in healthcare facilities: A harbinger of the future? Perspectives in Health Information Management, pp.1-22.

Stritch, M.M., Winterburn, M. & Houghton, F., 2021. The Conti ransomware attack on healthcare in Ireland: Exploring the impacts of a cybersecurity breach from a nursing perspective. Canadian Journal of Nursing Informatics, 16(3-4).

Snyder, H., 2019. Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, pp.333–339.

Steffen, E., Lyons, E. & Coyle, A., 2016. Ethical considerations in qualitative research. In Analysing Qualitative Data in Psychology, 2nd ed., pp.31–44.

Thamer, N., and R. Alubady. 2021. "A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research." 2021 1st Babylon International Conference on Information Technology and Science (BICITS), 210-216.

Tranfield, D., Denyer, D. & Smart, P., 2003. Towards a methodology for developing evidence-informed management knowledge by means of systematic review. British Journal of Management, 14(3), pp.207–222.

Tully, J., Selzer, J., Phillips, J.P., O'Connor, P. & Dameff, C., 2020. “Healthcare challenges in the era of cybersecurity.” Health Security, 18(3), pp.228–231.

Wheeler, T. & Alderdice, J.L., 2022. Cyber collateral: WannaCry & the impact of cyberattacks on the mental health of critical infrastructure defenders. *Changing Character of War Centre (CCW)*.

Wirth, A., 2018. The times they are a-Changin': Part two. *Biomedical Instrumentation & Technology*, 52(3), pp.236-240.

Zarocostas, J. (2021). "Health under cyberattack." The Lancet 398 (10303): 829-830.