Financial Impact of Ransomware and Malware in the Healthcare Sector

Introduction

The healthcare sector worldwide has a growing issue of ransomware and malware attacks which are having financial repercussions on the sector as a whole as they become a prime target. They are particularly vulnerable because they rely on a lot of data related to patient health, important IT infrastructure and because the healthcare sector is so critical being what the difference between a life being saved or not bad actors will take advantage of this. The financial repercussions can be devastating as not only if they pay the ransom, but also fines for data leaks. This literature review will dig into the impact of these financial costs and the impact this has on the healthcare sector covering the availability of literature and will lead to discussion on what needs to happen to make healthcare systems more secure to help prevent the costs of ransomware and malware attacks on the healthcare sector.

Background and Definitions

“An attack that occurs when hackers gain control of data or a computer system and hold it hostage until a ransom is paid. This can put your patients in danger and prevent you from delivering care in a timely fashion.” (Healthcare & Public Health Sector Coordinating Council, 2023). This is an attack is defined by the Healthcare & Public Health Sector Coordinating Council, a council formed of private healthcare companies and the Department of Health & Human Services, that have identified as one of the five current threats to the healthcare sector in their Health Industry Cybersecurity Practices (Healthcare & Public Health Sector Coordinating Council, 2023). This ransom is paid by cryptocurrency and more commonly bitcoin as the “transactions [are] easy while protecting the anonymity of those involved, it has

become the preference currency for criminal activity including ransomware hackers" (Paul et al, 2018) making it harder for the police to track who criminals are in time for the files to no longer be held ransom leading to the ransom being paid.

Financial Impact Literature

This section will cover current literature on financial impacts can be broken down into direct and indirect financial costs that impact the healthcare sector and its stakeholders. There will also be a comparative analysis with other sectors that have also had a financial impact from ransomware and malware attacks.

Direct Financial Impact

According to the Cyber Threat Intelligence Integration Centre, an office of the Director of National Intelligence, from 2022 to 2023 ransomware attacks on the healthcare sector doubling globally with the US healthcare sector increasing by 128% (Cyber Threat Intelligence Integration Centre, 2024). The direct financial impacts start with US hospitals having to delay procedures, having a disruption in patient care and the need to reschedule medical appointments until they pay or bypass the ransom. Sophos, a leader in cybersecurity solutions, reported that the average cost of a ransomware attack in 2024 was $2.57 million being double from 2021 with 57% of healthcare institutions paying the ransom being paid by the insurance providers of these institutions (Sophos, 2024).

Indirect Financial Impact

"Paying the ransom is often far cheaper than paying the restoration costs and business interruption costs also covered under the policy, there is an increased

tendency to pay the ransom" (Logue & Shniderman, 2021). Giving into the attackers can be seen as the easiest solution to keep business going and with the cost of recovering from data backups being more expensive allowing the healthcare providers insurance pay the ransomware cost is often the easiest solution as this contains patient data a lot of the time needing to protect this is a priority (Logue & Shniderman, 2021). This leads onto one of the first indirect financial impacts with the increase in insurance premiums for the healthcare sector as the attackers understand that is easier and cheaper to pay the ransom as the insurance provider will cover it allowing "insurers [to] sell more policies for higher premiums than before" (Logue & Shniderman, 2021). This leads to an overall indirect long-term financial impact of increased insurance premiums making the cost of paying the ransom more expensive. This insurance often does not cover the loss of revenue due to the downtime caused by the attack which would require a more complex policy as insurance evolves (Branch et al., 2019).

If a healthcare institution chooses not to pay the ransom and goes through the data restoration route which is reasonable to not want to pay the ransom ends up having consequences as the Health Insurance Portability and Accountability Act (HIPAA) which protects patient data. The attackers extract patient data before locking down the hospitals systems and if the hospital refuses to pay the ransom the data ends up being leaked which makes them in violation of HIPAA leading to a further long-term impact of reputational damage to the healthcare institution due to data leaks from ransomware (Kiser & Maniam, 2021).

Comparative Analysis

In comparison to other sectors healthcare is not the most targeted, ranking fourth, as the commercial sector suffered almost quadruple the attacks that the healthcare sector did in 2023 worldwide with financial being second and IT being third (Cyber Threat Intelligence Integration Centre, 2024). Despite the healthcare sector ransomware attacks not being the highest on the Cyber Threat Intelligence Integration Centre still revealed that all sectors experienced an increase in ransomware attacks showing it is a problem across all sectors.

What causes this Financial Impact?

Regulatory Body Fines

Regulatory bodies, as mentioned in the indirect costs section, is one of the factors that keep healthcare institutions that helps to protect patient data and issues penalties such as HIPAA (HIPAA Journal, 2024) and GDPR (European Parliament and Council, 2016). Where companies, in this case healthcare, can be penalised if they do not follow data protection standards leading to fines as large as 1.5 million euros, in the case of Dedalus Biologie who breached the data of 500,000 people because they breached GDPR. HIPAA in 2024 issued a fine of $90,000 to the Bryan County Ambulance Authority in Oklahoma as they had “never conducted a risk analysis to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI, and the seriousness of the violation warranted a financial penalty” (Alder, 2024) this exposed 14,273 patients and could have been avoided if they took the right preventative measures to protect their patient data. The benefit of these fines is that these penalties do not standalone and do come with the need to take corrective action and be monitored (Alder, 2024).

Preventative Measures

Following on from regulatory body fines, implementing preventative measures can ensure that they are not fined. Prospect Medical Group were hit hard as their 16 hospitals and 166 outpatient clinics across the US were shut down with ambulances having to go to other hospitals putting lives at risk (Carter, 2023). With training staff in cybersecurity is a great starting point to prevent these issues and with the implementation of protections advised by the Department of Health and Human Services can help protect from HIPAA fines and ransomware payments (Carter, 2023). Finally, operating on a “zero trust model” by cutting down on who has access to data can go a long way in preventing data leaks (Carter, 2023).

Alternate Views on Financial Impact of Ransomware and Malware Attacks

Smaller Institutions and Cost-Effective Cybersecurity

Ransomware attacks are not all encompassing as smaller institutions can often struggle most when such an attack occurs as bigger institutions can pay the ransom. This is why smaller institutions should be more willing to invest in preventative methods as this would help them reduce costs in the long-term as they would be able to reduce their risk profile when it comes to insurance and get a better rate allowing them to invest more in their IT infrastructure (Fallin, 2024).

Comparative Costs of Prevention compared to Recovery

Prevention can often be seen as expensive as it is a large cost upfront cost which is harder to justify which is why recovery and paying the ransom is often favoured as it is cheaper when it occurs. However, the hidden costs such as the cost of system outages have not been fully measured as the greater cost of paying the ransom in the long-term (Allcock, 2024). The benefits of paying a large amount upfront to prevent future attacks assists in preventing an increase in operational costs during

downtime, more preparation for these types of attacks and the maintaining of patient trust in the long-term (Allcock, 2024). This prevents being found in breach of charges regulations such as HIPAA which can only add to the long-term costs of not implementing preventative methods sooner.

Limitations in Current Literature

Gaps

The current gaps in literature related to the financial impact are that there currently is not enough studies into the long-term financial cost of ransomware and only mentions that it is an issue but not exactly how big of an issue it actually is. An extension of the aforementioned indirect costs of ransomware is that we do not know how much it costs the healthcare sector when medical procedures are delayed and appointments being pushed back with there being “no systematic documentation of the extent and effect of ransomware attacks on health care delivery organisations” (Barry, 2023). Additionally, there are a lot of individual case studies on a per hospital basis but not a bigger figure leading to “gaps in our understanding of the total problem” (Barry, 2023).

Suggestions

Further research that needs to be done in the area that would prove beneficial is an investigation into the indirect financial costs of ransomware and the tracking of increase of average insurance premiums in the healthcare sector to represent the total problem. More research into the reason why the rate of preventative measures is being outpaced by the increase of ransomware attacks with these attacks having doubled from 2022 to 2023. In general, there should also be more research over

time to review these attacks long-term after the attack such as the reputational damage.

Conclusion

In conclusion, the financial impact of ransomware and malware in the healthcare sector has both direct and indirect impacts with the direct impacts being paying the ransom or having to pay for the data backup restoration if the ransom is not paid which can be in the millions of dollars. The indirect costs being identified as being the increase in insurance premiums, the operation costs for delayed medical procedures and penalties related to violating regulatory body rules such as HIPPA showing that there is a gap in literature related to the long-term impacts after a ransom is paid. The other critical issue is the rate at which these attacks are increasing as they had doubled within a year from 2022 to 2023. With these attacks occurring more frequently at such a rate preventative measures need to be put in place such as increasing training with attacks being able to occur from simply clicking on a link or an attachment in an email leading to an outage costing the healthcare sector millions. However, this must be supported by improved IT infrastructure which makes it harder for links and attachments to be able to infect healthcare systems as well as making it harder for these attackers to extract patient data as well as locking down their systems. Finally, research into this area is important for long-term research into this area to have useful longitudinal data so that the indirect impacts can be measured to get accurate data on the financial losses as this would allow for more refined insurance policies that the healthcare sector can be protected by.

Reference List

Alder, S. (2024) *OCR Announces First Financial Penalty Under HIPAA Risk Analysis Enforcement Initiative*, *HIPAA Journal*. Available at: https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/ (Accessed: 02 November 2024).

Allcock, S. (2024) *The hidden costs of Ransomware: Why prevention is worth the investment*, *Financial News*. Available at: https://www.financial-news.co.uk/the-hidden-costs-of-ransomware-why-prevention-is-worth-the-investment/ (Accessed: 26 October 2024).

Barry, C. (2023) *Trends and data gaps revealed in New Healthcare Ransomware Attack Study*, *Barrcuda Blog*. Available at: https://blog.barracuda.com/2023/05/16/healthcare-ransomware-attack-study (Accessed: 20 October 2024).

Branch, L.E. *et al.* (2019) 'Trends in malware attacks against United States Healthcare Organizations, 2016-2017', *Global Biosecurity*, 1(1), p. 15. doi:10.31646/gbio.7.

Carter, C. (2023) *Cyber attacks in healthcare can be deadly. here are 3 ways to prevent them*, *World Economic Forum*. Available at: https://www.weforum.org/stories/2023/08/3-ways-prevent-cyber-attacks-improve-healthcare-outcomes/ (Accessed: 20 October 2024).

Cluley, G. (2021) *Insurer AXA says it will no longer cover ransomware payments in France*, *Bitdefender*. Available at: https://www.bitdefender.com/en-au/blog/hotforsecurity/insurer-axa-says-it-will-no-longer-cover-ransomware-payments-in-france (Accessed: 20 October 2024).

Cyber Threat Intelligence Integration Centre (2024) *Ransomware attacks surge in 2023; Attacks on Healthcare Sector Nearly Double*. Available at: https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf (Accessed: 15 October 2024).

EDPB (2022) *Health Data Breach: Dedalus Biologie fined 1.5 million euros*, *Health data breach: Dedalus Biologie fined 1.5 million euros | European Data Protection Board*. Available at: https://www.edpb.europa.eu/news/national-news/2022/health-data-breach-dedalus-biologie-fined-15-million-euros_en (Accessed: 20 October 2024).

European Parliament and Council (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Official Journal of the European Union L119, pp. 1–88. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (Accessed: 20 October 2024)

Fallin, C. (2024) *Navigating cybersecurity on a tight budget: Strategies for healthcare leaders*, *Burwood Group*. Available at: https://www.burwood.com/blog-archive/navigating-cybersecurity-on-a-tight-budget-strategies-for-healthcare-leaders (Accessed: 20 October 2024).

Healthcare & Public Health Sector Coordinating Council (2023) *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*. Department of Health and Human Services (DHHS).

Joshi, A. (2024) *These are the biggest cybercrime targets, and other cybersecurity news to know this month*, *World Economic Forum*. Available at:

https://www.weforum.org/stories/2024/04/cybercrime-target-sectors-cybersecurity-news/ (Accessed: 14 October 2024).

Kiser, S. and Maniam, B., 2021. Ransomware: Healthcare industry at risk. Journal of Business and Accounting, 14(1), pp.64-81.

Logue, K.D. and Shniderman, A.B. (2021) 'The case for Banning (and mandating) ransomware insurance', *SSRN Electronic Journal* [Preprint]. doi:10.2139/ssrn.3907373.

Paul III, D.P., Spence, N., Bhardwa, N. and Coustasse, A., 2018. Healthcare Facilities: Another Target for Ransomware Attacks.

Sophos (2024) *Two-Thirds of Healthcare Organizations Hit by Ransomware – A Four-Year High, Sophos Survey Finds*, *Sophos*. Available at: https://www.sophos.com/en-us/press/press-releases/2024/04/ransomware-payments-increase-500-last-year-finds-sophos-state (Accessed: 15 October 2024).