USING MACHINE LEARNING TO CREATE AN INTRUSION DETECTION SYSTEM TO DETECT RANSOMWARE ATTACKS

EFFECT OF CYBER INSURANCE ON HOSPITAL CYBERSECURITY

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Feyona Zhang

December 14, 2024

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

Kent Wayland, Department of Engineering and Society

Rosanne Vrugtman, Department of Computer Science

General Problem

How can we prevent ransomware attacks with machine learning and increase the cybersecurity practices of hospitals with cyber insurance?

Ransomware is a form of malware that locks a person out of their device or system until a ransom is paid to the attacker. In recent years, attacks have evolved to have an additional phase where sensitive information is exfiltrated for ransom (Cartwright et al., 2023). Each year, ransomware costs businesses and governments hundreds of millions of dollars, and high profile incidents have resulted in the U.S. Department of Justice to categorize ransomware attacks on the same level of concern as terrorist attacks (Yilmaz et al., 2023). The government response will not be addressed in this study, but given the severity and rapid evolution of ransomware, it is critical to investigate how to prevent ransomware attacks.

A key factor in the success of these attacks is the decision to pay the ransom, which often occurs when the cost of the information ransomed and disruptions to normal operations are deemed greater than the cost of the ransom payment. Critical infrastructures, such as hospitals and power grids, are especially vulnerable because of the essential role they play in society and their need for immediate access to information.

Tackling the challenge of preventing ransomware attacks can be approached in two ways. My technical project will explore how machine learning algorithms can be applied to monitor a system to detect attacker infiltration. At the same time, employing a machine learning defense strategy comes with broader socio-technical implications concerning the environment it is deployed in and the social groups involved. As such, my sociotechnical project will explore how cyber insurers influence the cybersecurity practices and dynamics within an organization with regards to ransomware. These two approaches, when applied together, develop a technique to

prevent ransomware attacks and explore the dynamics within the organizations that are vulnerable to them.

Using Machine Learning to Create an Intrusion Detection System to Detect Ransomware Attacks

How to prevent ransomware infiltration with machine learning monitoring of a system?

Currently, network monitoring of a system to detect ransomware attacks is done by detecting unusual patterns of behavior through an intrusion detection system (IDS). An IDS will create an alert for people to view and determine whether the activity is malicious. Cybersecurity experts can be inundated with thousands of alerts without a way to view them all, inducing alert fatigue. Algorithms have been produced to filter out some of the false positives and true negatives, however, more can be done to create a system that detects malicious activities that indicate a ransomware attack. My technical research will address this gap by training a machine learning algorithm to learn the correct patterns of behavior tailored to a specific system within a hospital. This will relieve the stress of millions of false positive reviews by human administrators and more accurately detect true ransomware activity.

Hospitals are acutely vulnerable to ransomware attacks due to their reliance on information and large attack surface through Internet of Things (IoT) devices. Since their exposure surface is vast, there has been research identifying vulnerable points within hospitals. Yu and Wei (2023) identified hospital websites as having multiple network security vulnerabilities which allow attackers to infiltrate and exploit through social engineering. In addressing IoT devices, there has been proposed research to create a lightweight IDS for IoT devices using machine learning algorithms, however, it has not been fully implemented or deployed to an actual hospital system (Mofidi, Hounsinou, & Bloom, 2023). From the current

literature, it can be seen that hospitals have multiple fronts of exposure to ransomware attacks which can be addressed. My research will aim to create a machine learning model that will counter the poor cybersecurity practices that researchers have identified within hospitals to prevent ransomware attacks.

I will create a machine learning model that monitors a hospital system and is trained on preprocessed user activity and correct operation of IoT devices in a hospital. My model will predict whether network activity or IoT operation data in a hospital is malicious or not. First, I will gather the relevant information from hospitals. Next, I will prepare the data through data cleaning and feature engineering to get rid of null values and features with low correlation. To train the model, I will apply boosting, decision tree, and random forest to predict the activity in a hospital as either malicious or non-malicious. With the model created and trained, it will be further fine-tuned as more hospital data is collected and added. Finally, the model will be assessed based on its prediction accuracy. When the model is trained to a sufficient prediction accuracy, it will be ready to be tested on testing data and real hospital systems. The machine learning model created at the end of this study will more accurately identify cybersecurity threats than current technologies and allow hospitals to address malicious behavior.

Effect of Cyber Insurance on Hospital Cybersecurity

How does a cyber insurer influence the change in the cybersecurity system and dynamics within a hospital to prevent ransomware attacks?

Introduction

Critical infrastructure includes hospitals, transportation, utilities, and power grids. The focus of my research will be ransomware attacks on hospitals. Since hospitals are migrating much of their data into online systems to make them more accessible (Hatzivasilis et al, 2020),

hospitals are acutely vulnerable through these avenues of entry in IoT devices and online systems. When a ransomware attack is performed on a hospital, this can involve the compromise of millions of patients' personal information. In response to rapidly developing ransomware technology and moving data online, hospitals have taken measures to increase their cybersecurity and protect themselves through cyber insurance.

Background

Cyber insurance pools risks and limits the exposure of organizations (Cartwright et al, 2023). Being a relatively new type of insurance, cyber insurance policies are slowly being developed to encompass the wide range of cybersecurity risks in different industries. Currently, there is a lack of government oversight over cyber risks, allowing cyber insurance providers to develop their own policies and, as a result, to act as a regulatory power over the security practices of the organizations they insure. When an organization contracts with a cyber insurance company, the organization's cybersecurity practices are being co-regulated as the cyber insurance company only insures companies that meet a certain cybersecurity standard.

Due to the infancy of the cyber insurance industry, there have been issues of cyber insurance being largely ineffective at regulating an organization's cybersecurity policies due to lack of actuarial data. (Hatzivasilis et al., 2020). In another study, Li and Liao (2023) showed that while cyber insurance benefits the insured in a financial way, it may not benefit the overall cybersecurity practices of society due to decreasing investments in cybersecurity practices if an organization is covered by cyber insurance and risk management services.

However, Hatzivasilis et al. (2020) showed that the interaction between cyber insurance companies and the organizations they insure will generate more statistical data to improve cybersecurity practices, and, in turn, grow the cyber insurance market in maturity. A case study

in Singapore revealed that standardizing the taxonomy for describing cybersecurity incidents, creating a database of incidents and losses, and benchmarking different models with actuarial pricing can successfully align incentives, and Singapore was able to successfully develop a $1 billion cyber risk pool (Talesh, 2022). This shows that the causal relationship between cyber insurance companies and the organizations they insure can potentially have a positive effect on an organization's ability to repel ransomware attacks. With this knowledge, more can be explored on the actual effects of cyber insurance on specific hospitals.

Cyber insurers and cybersecurity practices highlight a mutually formative relationship where in response to ransomware attacks, hospitals employ cyber insurance to address cyber risks, and in turn, their cybersecurity practices are shaped by cyber insurance. Because hospitals are a frequent target of ransomware attacks, it will be useful to examine how cyber insurance can have a strengthening effect on hospital cybersecurity.

Literature Review

In current literature, Hatzivasilis et al. (2020) describe a cyber insurance framework, CyberSure, which can be applied to the healthcare sector due to its dynamic policies that adjusts its cyber policies, premiums, and risk assessments as new data is being added into the system. Thus, cyber insurance has developed to the point of being readily adapted and provided to the healthcare sector, however, it can be further studied the effects of its actual implementation in hospitals. Jalali and Kaiser (2018) investigated the current cybersecurity practices and dynamics within a hospital and broadly across the US. While their study provides a general overview of hospital cybersecurity, more can be researched about the impact of cyber insurance on the socio-technical dynamics within a hospital. In their study, Munoz Cornejo, Lee, & Russell

(2024) concluded that the prevalence of ransomware attacks targeting hospitals highlights vulnerabilities and the critical need for enhanced security measures.

Cyber insurance has been shown to decrease the likelihood that organizations pay the ransom, but limited research has been done on the impact of cyber insurance on hospital cybersecurity practices. This shows a gap in knowledge in how cyber insurance can improve the cybersecurity of hospital systems to prevent ransomware attacks. I will frame my research with the social construction of technology (SCOT) theory, considering how cyber insurance and hospital cybersecurity practices cocreate one another.

Methods

My research will apply the social construction of technology framework to explore how hospitals' cybersecurity practices are shaped by cyber insurance policies and reflect negotiated understandings of security, risk, and responsibility (Johnson, 2005). To address my research question, I will consult various stakeholders and analyze case studies and policies. I will interview the expert opinions of chief information officers (CIOs), chief information security officers (CISOs), and health care cybersecurity experts in hospitals. From the interviews, I will be able to learn about the shifts and stabilization of cybersecurity practices within hospitals in response to ransomware and various interest groups. Similarly, case studies of ransomware attacks on hospitals will provide information on how a hospital might change their cybersecurity practices after an attack reveals vulnerabilities in their system, leading to stabilization of the hospital cybersecurity socio-technical infrastructure. Through reading cyber insurance policies, I will be able to understand the potential influence cyber insurers have as a relevant social group on encouraging secure cyber practices in the organizations they insure. Finally, I will research government policies to understand what hospitals are required to do by law to mitigate

ransomware attacks. This methodology will allow me to highlight how cybersecurity in hospitals is interpreted and reshaped by hospitals, cyber insurers, government regulators, and attackers (Pinch & Bijker, 1987). Since cybersecurity against ransomware is shaped by social, economic, and institutional forces, using the SCOT framework, I can investigate how cyber insurance policies and hospital cybersecurity practices are co-constructed in response to ransomware attacks.

Conclusion

In conclusion, as ransomware becomes a more prevalent issue in society, it is important to explore how critical system infrastructures are developing their cybersecurity policies to mitigate the significant damage induced by these attacks. My technical research will aim to address cybersecurity vulnerabilities in hospitals by creating a machine learning algorithm that will detect malicious activity and improve the threat review process. This research will help accelerate the adaptation of greater cybersecurity measures in hospitals to address the growing frequency of ransomware attacks. At the same time, my STS research will apply the SCOT framework to cyber insurance in hospitals to create a novel study on how cyber insurance can shape and is shaped by hospital cybersecurity. Given the significance of ransomware attacks on critical infrastructure, the results of these two studies will contribute to the prevention and understanding of ransomware and hospitals in an effort to shape the optimal cybersecurity practices to protect our critical systems.

References

Baker, T., & Shortland, A. (2023). The government behind insurance governance: Lessons for ransomware. Regulation & Governance, 17(4), 1000–1020. https://doi.org/10.1111/rego.12505

Cartwright, A., Cartwright, E., MacColl, J., Mott, G., Turner, S., Sullivan, J., & Nurse, J. R. C. (2023). How cyber insurance influences the ransomware payment decision: theory and evidence. Geneva Papers on Risk & Insurance, 48(2), 300-331. https://doi.org/10.1057/s41288-023-00288-8

Hatzivasilis, G., Chatziadam, P., Miaoudakis, A., Lakka, E., Ioannidis, S., Alessio, A., Smyrlis, M., Spanoudakis, G., Yautsiukhin, A., Antoniou, M., & Stathiakis, N. (2020). Towards the insurance of healthcare systems. In A. P. Fournaris, M. Athanatos, K. Lampropoulos, S. Ioannidis, G. Hatzivasilis, E. Damiani, H. Abie, S. Ranise, L. Verderame, A. Siena, & J. Garcia-Alfaro (Eds.), Computer Security (pp. 185–198). Springer International Publishing. https://doi.org/10.1007/978-3-030-42051-2_13

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. Journal of Medical Internet Research, 20(5), e10059. https://doi.org/10.2196/10059

Johnson, D. (2005). Social construction of technology. In C. Mitcham (Ed.), *Encyclopedia of Science, Technology, and Ethics* (Vol. 4, pp. 1791–1795). Macmillan Reference.

Li, Z., & Liao, Q. (2023). Does cyber-insurance benefit the insured or the attacker? – A game of cyber-insurance. In J. Fu, T. Kroupa, & Y. Hayel (Eds.), *Decision and Game Theory for Security* (pp. 23–42). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-50670-3_2

Mofidi, F., Hounsinou, S., & Bloom, G. (2023). L-IDS: A lightweight hardware-assisted IDS for IoT systems to detect ransomware attacks. Proceedings of the 8th ACM/IEEE Conference on Internet of Things Design and Implementation, 464–465. https://doi.org/10.1145/3576842.3589170

Munoz Cornejo, G., Lee, J., & Russell, B. A. (2024). A thematic analysis of ransomware incidents among United States hospitals, 2016–2022. Health and Technology, 14(6), 1059–1070. https://doi.org/10.1007/s12553-024-00890-3

Pinch, T. F., & Bijker, W. E. (1987). The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. In W. E. Bijker, T. P. Hughes, & T. F. Pinch (Eds.), *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (pp. 17–50). MIT Press.

Talesh, S. (2022, November 4). Cyber insurance and cybersecurity policy: An interconnected history. Lawfare. https://www.lawfaremedia.org/article/cyber-insurance-and-cybersecurity-policy-interconnected-history

Yilmaz, Y., Cetin, O., Grigore, C., Arief, B., & Hernandez-Castro, J. (2023). Personality types and ransomware victimisation. *Digital Threats*, 4(4), 53:1-53:25. https://doi.org/10.1145/3568994

Yu, Y., & Wei, Y. (2024). Hospital website penetration analysis and vulnerability reproduction method. *Proceedings of the 2023 International Conference on Power, Communication, Computing and Networking Technologies*, 1–5. https://doi.org/10.1145/3630138.3630461