Cybersecurity and Ransomware

Julia Calabrese

Computer Information Systems, Post University

CIS 311: Technical Writing in CIS

Dr. Schwartz

12/7/2025

Executive Summary

Ransomware has been one of the most severe cybersecurity threats in recent years. It can financially harm and damage an organization's reputation. This report evaluates several preventative strategies for ransomware to protect against it. These strategies include time-series analysis, blockchain, and cyber insurance. Each strategy offers its own unique techniques, including trend analysis, encryption and authentication protocols, and external protection.

The findings determine that these strategies are effective in preventing ransomware attacks. Time-series analysis identifies risks and vulnerabilities in information security programs through trend analysis. Blockchain requires access controls to access the encrypted data. Cyber Insurance performs risk assessments to identify vulnerabilities in the information security system that need to be addressed.

Additionally, this report determines an answer to the long-term debate of whether or not ransom payment should be fulfilled. Each side has their own advantages and disadvantages. Various advantages of fulfilling payment are minimal business interruption and faster recovery. However, the risks include a poor reputation, financial loss, increased attacks, and data that cannot be fully recovered. On the other hand, unfulfilling payment decreases the risk of further attacks, complies with legal and ethical guidelines, and discourages cybercriminals. However, the risks include poor reputation, financial loss, long-term business interruption, and unrecovered data. In comparison, it is beneficial not to fulfill the ransom payment because of compliance with legal and ethical guidelines, and to prevent future attacks for the organization and others.

Overall, this analysis suggests utilizing the preventative strategies from the findings and not fulfilling the ransom payment. Utilizing preventative strategies mitigates the risk of ransomware attacks, which can be detrimental to an organization. In the case that an organization is attacked with ransomware, it is recommended not to engage with cybercriminals and not to fulfill the payment.

Introduction

Ransomware has become a trending cyber-attack that has impacted all industries over the past decade (MacColl et al., 2023). Hackers collect sensitive data and request compensation for the organization to regain access. Typically, the compensation is a monetary payment known as ransom. As these attacks are increasing in frequency and sophistication, it is crucial for organizations to implement preventive measures to remain unaffected. This report reviews effective preventive strategies, such as time-series analysis, blockchain, and cyber insurance. Additionally, the effectiveness of their efforts in preventing ransomware attacks. Furthermore, the analysis examines whether ransom payments should be made in the event of an attack.

Methodology

This report uses a qualitative research approach to determine prevention, its effectiveness, and the advantages and disadvantages of payment for ransomware. The information was collected from public databases such as ERIC, JSTOR, and ProQuest. The analysis was conducted based on articles pertaining to real-world ransomware attacks and unique strategies to prevent and mitigate ransomware and cyberattacks. The findings were examined using comparative analysis to evaluate the effectiveness of each strategy. Additionally, the advantages and disadvantages of ransom payment were assessed using the same analytical approach, simultaneously with risk-benefit analysis.

Findings

Prevention Strategies

Time-Series Analysis

Time-series analysis is the extraction of time-ordered information using statistical methods (Roumani, 2025). This analysis employs a formula that incorporates the elements of trend (T), seasonality (S), residuals (R), series (Y), and time (t). The trend, seasonal, and residuals of time are the sum of Y of time ($Y_t = T_t + S_t + R_t$). This formula extracts seasonal and trending data in unison by calculating residual and unaccounted noise within ransomware data. Additionally, this formula incorporates local scatterplot smoothing (LOESS) (Roumani, 2025). LOESS is a method used to produce clear estimates that improve the results of time-series analysis formulas.

Time-series analysis is effective in protection due to its detection capabilities. Time-series analysis detects unusual activity based on time and trend. Based on the industry the organization is in, the time period of attacks that happened is displayed. In return, demonstrating when ransomware attacks are likely to occur. Additionally, time-series analysis can reveal vulnerabilities in an information security plan and identify areas that need improvement to further prevent attacks.

Blockchain

Blockchain is a distributed database technology where data is stored and managed in a peer-to-peer (P2P) network (Ryu, Kim, 2025). Blockchain ensures high quality data management and security through data storage on multiple devices in the P2P network. A blockchain consists of various blocks. Each block contains a header and a data record. Within the header contains a hash value. The hash value in each record is duplicated into the next header to link the blocks together. This process ensures the confidentiality, integrity, and availability of data is upheld.

Blockchain is effective in preventing ransomware due to its encryption and authentication protocols. Blockchain utilizes various keys to encrypt the data within the blocks. This creates a challenge for hackers to read the data, which reduces the risk of a ransomware attack. To further enhance security, blockchain requires authentication to access data. Blockchain utilizes authentication and verification protocols, such as two-factor authentication, to access the encrypted data.

Cyber Insurance

Cyber Insurance is a method of risk transfer that provides protection from cyber threats to businesses (Degefu, 2025). Cyber Insurance is where a third party is relied on to perform cybersecurity operations. These organizations will conduct a risk assessment of the organization to identify the risks and vulnerabilities that need to be addressed (MacColl et al., 2023). The risk assessment can be done through questionnaires or an external network scan of their IT infrastructure.

Cyber insurance is effective in preventing ransomware because it detects current risks and vulnerabilities prior to an attack. They can be patched and monitored by the insurance organization. Additionally, partnering with an organization to protect and monitor your assets provides further protection. Cyber insurance is an external party that specializes in cybersecurity and has the capabilities that several organizations do not. They provide an extra layer of protection while simultaneously monitoring your information and assets.

Advantages and Disadvantages of Ransom Payment

When attacked with ransomware, organizations face a difficult decision about whether to fulfill the ransom payment. The benefit of paying ransom is that business interruption is minimized, and recovery time is quicker. On the other hand, the organization risks gaining a poor reputation with consumers, financial loss for the company, increased risk of additional attacks, unsecure recovered data, and unpromised data recovery (Turrell, Boulanin, 2020). Additionally, ransom payment creates a risk to other organizations falling victim to ransomware.

On the other hand, there are advantages and disadvantages to not fulfilling the ransom payment. The benefits include decreasing the risk of future attacks, compliance with cyber legal and ethical guidelines, and discouraging cybercriminals (MacColl et al., 2023). Meanwhile, the risks include minimal data recovery, a poor reputation due to stolen data, financial loss to consumers, and long-term business interruption.

Using comparative analysis, it is more beneficial not to pay ransom for ransomware. Not paying for ransomware prevents further attacks that could impact the organization’s finances and operations. Additionally, it complies with legal and ethical guidelines. If ransom payment is fulfilled, it provides criminals with encouragement and financial gain. Cyber criminals should never be engaged with, nor encouraged to continue their illegal attacks.

Conclusion

In summary, time-series analysis, blockchain, and cyber insurance are effective preventive strategies to prevent ransomware attacks. Time-series analysis detects unusual and suspicious activity based on trend patterns that identify which countermeasures should be implemented. Blockchain encrypts sensitive data and requires authentication and verification access controls. Cyber insurance provides an additional layer of protection by utilizing an external source to assess, monitor, and mitigate the risks and vulnerabilities that an organization may have. In the case that an organization is attacked with ransomware, the ransom payment should not be fulfilled. Not fulfilling compensation decreases the risk of future attacks within the organization and other organizations, complies with legal and ethical guidelines, and discourages cybercriminals. When working in the cybersecurity field, it is unethical to comply with cybercriminals to uphold the confidentiality, availability, and integrity of the information.

References

Chinthapalli, K. (2017). The hackers holding hospitals to ransom. *BMJ: British Medical Journal*, *357*. JSTOR. https://doi.org/10.2307/26944485

Degefu, M. W. (2025). *Challenges Microbusinesses Face in Managing Cyber Risk: A Qualitative Analysis Exploring Cyber Insurance as a Response to Cyber Risk - ProQuest*. Proquest.com. https://www.proquest.com/docview/3201274791/DB9CD73972514117PQ/73?sourcetype=Dissertations%20&%20Theses

Ferdous, J., Islam, R., Mahboubi, A., & Islam, M. Z. (2025). A novel technique for ransomware detection using image based dynamic features and transfer learning to address dataset limitations. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-025-17647-1

Ghulam, M. (2025). *Date of Finalization of Manuscript*. https://files.eric.ed.gov/fulltext/ED675147.pdf

Harding, E., & Ghoorhoo, H. (2022). *Hard Choices in a Ransomare Attack*. Center for Strategic and International Studies (CSIS); JSTOR. http://www.jstor.org/stable/resrep43414

MacColl, J., Sullivan, J., Jason, Turner, S., Mott, G., Cartwright, E., & Cartwright, A. (2023). The Role of Cyber Insurance in the Ransomware Business Model. In *Cyber Insurance and the Ransomware Challenge* (pp. 22–43). Royal United Services Institute (RUSI); JSTOR. http://www.jstor.org/stable/resrep71669.7

Ryu, J., & Kim, T. (2025). Enhancing Hospital Data Security: A Blockchain-Based Protocol for Secure Information Sharing and Recovery. *Electronics*, *14*(3), 580. https://doi.org/10.3390/electronics14030580

TURELL, J., SU, F., & BOULANIN, V. (2020). Lessons from past cyber incidents and country studies. In *Cyberincident Management* (pp. 32–42). Stockholm International Peace Research Institute; JSTOR. http://www.jstor.org/stable/resrep26199.11

Wang, P., Lin, H.-C., Chen, J.-H., Lin, W.-H., & Li, H.-C. (2025). Improving Cyber Defense Against Ransomware: A Generative Adversarial Networks-Based Adversarial Training Approach for Long Short-Term Memory Network Classifier. *Electronics*, *14*(4), 810–810. https://doi.org/10.3390/electronics14040810

Yaman Roumani, & Roumani, Y. F. (2025). Predicting Ransomware Incidents with Time-Series Modeling. *Journal of Cybersecurity and Privacy*, *5*(3), 61–61. https://doi.org/10.3390/jcp5030061

Databases

ERIC. (n.d.). *ERIC - Education Resources Information Center*. Eric.ed.gov. https://eric.ed.gov

Jstor. (1999). JSTOR. In *Jstor.org*. https://www.jstor.org

ProQuest. (n.d.). *ProQuest | Databases, EBooks and Technology for Research*. Www.proquest.com. https://www.proquest.com