Mitigating Ransomware in Government-Managed Institutions: A Global Critical Information Infrastructure Perspective

Musiwalo Mashila, Siphesihle Philezwini Sithungu and Khutso Lebea
Academy of Computer Science and Software Engineering, Faculty of Science, University of Johannesburg, South Africa

220012036@student.uj.ac.za
siphesihles@uj.ac.za
klebea@uj.ac.za

Abstract: This paper examines the escalating ransomware threats faced by government-managed educational institutions, focusing on their vulnerabilities, case studies, and mitigation strategies. With the adoption of Bring Your Own Device (BYOD) policies, schools increasingly expose their networks to cyber risks, making them attractive targets for cybercriminals. Case studies, including attacks on the Los Angeles Unified School District and the University of California, San Francisco, illustrate the profound impact of ransomware incidents and the diverse responses of institutions. Effective cybersecurity measures are crucial, emphasizing the need for prioritized spending, comprehensive security training, and advanced detection and response strategies. The role of government is also vital, as it develops legislation, guidelines, and funding opportunities to enhance educational cybersecurity. Recommendations include technical measures to secure networks and collaborative educational initiatives to share best practices. Ultimately, this research study underscores the necessity of continuous adaptation and government support in fortifying defences against ransomware threats. By fostering a cybersecurity awareness and resilience culture, educational institutions can better protect sensitive data and ensure the safety of their operations in an increasingly tricky digital landscape.

Keywords: Ransomware, Educational institutions, Critical information infrastructure, Bring Your Own Device (BYOD)

1. Introduction

Protecting Critical Information Infrastructure (CII) is vital for national security and economic stability in our increasingly digitized world. The Information Technology Act of 2000 defines CII as "a computer resource, the incapacitation or destruction of which shall have a debilitating impact on national security, economy, public health, or safety" (Drishti IAS, 2022). This encompasses vital services, including telecommunications, financial systems, and the electric power grid (Chen, et al., 2024).

Government-managed educational institutions are among the sectors that play a crucial role in the CII (CISA, 2024). These institutions, ranging from preschools to higher education, hold vast repositories of sensitive data—student records, financial information, and research data—making them attractive targets for cybercriminals (Pandit, 2023). Education is recognized as a driver of economic growth, enhancing individual skills and productivity, fostering innovation, and supporting entrepreneurship. Education reduces poverty and drives economic diversification by equipping individuals with better job opportunities, ultimately boosting living standards and government revenue (Jahankhani, et al., 2023).

Ransomware poses a significant threat to IT users globally. This affects individuals, governments, and organizations (Zakaria, et al., 2017). Ransomware tactics continue to evolve despite the advances in cybersecurity. This makes educational institutions a consistent target alongside manufacturing and healthcare (Jahankhani, et al., 2023). This paper examines the ransomware threats facing government-managed educational institutions, analyzing attack types, execution methods, and impact. The paper further evaluates the role of government agencies in mitigating these threats and assesses the effectiveness of existing policies and frameworks. Finally, the study proposes strategies to enhance the resilience of critical entities as a contribution to ensuring their secure and effective operation.

This paper is structured as follows. Section 2 presents the problem background. Section 3 examines the threat of ransomware in government-managed educational institutions. Section 4 explores ransomware mitigation strategies, including the role of government in mitigating ransomware. Section 5 provides recommendations for minimising the risk of ransomware. Finally, Section 6 concludes the paper.

2. Problem Background

This section highlights the ransomware threat facing government-managed educational institutions and the need for solid protection strategies. It explains how ransomware works, its risks to essential services and sensitive data, and the government's role in securing information. Reviewing current defence methods such as

backups, antivirus updates, and awareness training, this section shows the importance of a well-rounded approach to cybersecurity. It sets the stage for discussing ways to improve ransomware defences in public institutions.

2.1 Overview of Ransomware Threats

Ransomware is malicious software that turns off a computer's functionality and demands payment for restoration (O'Gorman & McDonald, 2012). Early versions were rudimentary, but advances have led to sophisticated strains such as Cerber (Pletinckx, et al., 2018), TeslaCrypt (Lemmou & Souidi, 2018), and CryptoWall (Kara, et al., 2020). Despite the availability of decryption tools, recent ransomware has evolved into robust encryption applications resistant to analysis, with over 60 active families reported (O'Kane, et al., 2018).

Ransomware attacks typically progress through five distinct phases. In the initial phase, exploitation and infection, ransomware is delivered through phishing emails or exploit kits that take advantage of software vulnerabilities, as seen in the Angler exploit kit, which targets weaknesses in Adobe Flash and Internet Explorer. In the delivery and execution phase, ransomware establishes persistence mechanisms, often using encrypted channels to evade interception. It commonly places malicious files in folders like *%APPDATA%* or *%TEMP%,* enabling it to resume operations after a reboot. Following this, the backup spoliation phase involves ransomware deleting backup files soon after execution to impede recovery, with tools like *vssadmin* frequently used to remove volume shadow copies. In the file encryption phase, ransomware initiates a secure key exchange with its command and control (C2) server to obtain encryption keys, often utilizing robust encryption methods such as *AES-256*. Some variants may even handle encryption locally without contacting the C2 server. Finally, ransomware alerts the user by leaving a ransom note with payment demands in the user notification and clean-up phase, thereby completing the attack (Brewer, 2016).

2.2 Ransomware in the Education Sector

Ransomware directly impacts educational institutions by encrypting critical files and restricting access for staff and students. Infections can encrypt files within three seconds, highlighting the urgency for protective measures. For example, the Los Angeles Unified School District experienced a ransomware attack that exposed the sensitive health records of approximately 2,000 students, raising significant concerns over data security (Kapko, 2023). Similarly, the University of California, San Francisco, was targeted by a ransomware attack on its School of Medicine, where attackers deployed the NetWalker ransomware and demanded $1.14 million for decryption keys (Winder, 2020).

2.3 Government's Role in Critical Information Infrastructure Protection (CIIP)

While industry-led solutions are preferred, discussions on CIIP recognize the government's complex role. The government is crucial for bringing stakeholders together, encouraging information sharing, and financing long-term IT security research. However, it frequently faces criticism for lagging in technology and ineffectual legislation. Practical government actions include establishing market standards and providing safe harbours for data sharing, although these must serve the public interest to maintain trust (Cukier, et al., 2005).

In the UK, government-managed educational institutions must follow cybersecurity policies, including annual cyber risk assessments and cyber awareness plans. The Department of Education outlines guidelines for securing technology and data and reporting cyber-attacks (Department of Education, 2022). In South Africa, institutions must comply with the POPI Act, National Cybersecurity Policy Framework, and Cybercrimes Act, which collectively form a comprehensive framework for cybersecurity and data privacy (Charandura, 2022).

2.4 Existing Mitigation Strategies

Educational institutions employ several strategies to combat cybersecurity threats like ransomware, including regular data backups, updating antivirus software, and ongoing risk assessments. Emphasis on cybersecurity awareness through employee training and incident response practices is crucial. Institutions are increasingly adopting advanced technologies such as machine learning and honeypots to detect and prevent cyberattacks effectively. The effectiveness of these strategies varies based on resources and implementation efforts, underscoring the need for ongoing evaluation (Jahankhani, et al., 2023).

3. Ransomware Threats in Government-Managed Educational Institutions

This section examines the ransomware risks facing government-managed educational institutions, focusing on vulnerabilities, real-world case studies, and their broader implications. Analyzing the BYOD policies that increase exposure to attacks outlines the security challenges created by diverse devices on campuses. Case studies of the

Los Angeles School District and UCSF reveal the severe impact of ransomware on educational institutions, including data theft, high recovery costs, and difficult ethical decisions regarding ransom payments.

3.1 Vulnerabilities in Educational Infrastructure

Bring Your Own Device (BYOD) policies present significant vulnerabilities to the information infrastructure of educational institutions. As the variety of devices on campus increases, so do the risks of data breaches and cyberattacks. Security protocols must adapt to accommodate diverse devices, each with potential weaknesses. This diversity creates multiple entry points for cyber threats, heightening the exposure to attacks and unauthorized access to sensitive data (Nico, 2013; Grady, 2024).

3.2 Case Studies

Case Study 1: Los Angeles Schools District Attack

In 2022, a ransomware attack on the Los Angeles School District (LAUSD) resulted in the theft of thousands of files, which were subsequently released on the dark web. The compromised data included confidential psychological assessments, contract documents, and personal identifying information like Social Security numbers. Although the breach did not impact critical systems related to employee healthcare or school safety, the incident underscored the necessity for robust backup systems and incident response plans. LAUSD Superintendent Alberto Carvalho took a firm stance against negotiating with the attackers, describing their ransom demands as "absurd" and "insulting." (Jonathan, 2022).

This case study highlights the importance of robust backup systems, recovery plans, and collaboration with law enforcement. It also demonstrates the potential consequences of refusing to pay ransoms, including the risk of data leaks.

Case Study 3: University of California, San Francisco Attack

In 2020, hackers targeted the University of California, San Francisco (UCSF) using the NetWalker ransomware campaign, encrypting sensitive data within the School of Medicine. Although patient care and COVID-19 research were not affected, data on a limited number of servers was compromised. Initially demanding a ransom of $3 million, negotiations led UCSF to pay $1.14 million to recover the data, illustrating the high stakes in protecting critical research (Winder, 2020).

This case highlights the complex decision-making process when critical research data is at stake. It demonstrates the potential for successful negotiation with attackers and the high costs associated with ransomware attacks, even when paying the ransom.

Analysis and Implications

The ransomware incidents at LAUSD and UCSF reveal contrasting approaches to cybersecurity threats within government-managed educational institutions. LAUSD’s refusal to engage with cybercriminals reflects a commitment to ethical standards, prioritizing public trust over immediate recovery. Conversely, UCSF's decision to pay the ransom highlights the urgent need to protect vital research data, revealing the high costs of ransomware attacks.

Both cases underscore the necessity of comprehensive cybersecurity strategies tailored to the unique contexts of educational institutions. Implementing robust backup systems, incident response plans, and collaborative frameworks with law enforcement can enhance resilience against ransomware threats.

4. Ransomware Mitigation Strategies and Governmental Role

This section outlines key strategies for mitigating ransomware threats in educational institutions, highlighting the importance of governmental support and collaboration.

4.1 Mitigation Strategies

Preventive Strategies

Firstly, educational institutions need to prioritize cybersecurity-related spending. Colleges and universities have historically prioritized research, academics, and student aid over cybersecurity investments. As ransomware and malware attacks become more prevalent, institutions must allocate dedicated budgets to address escalating threats. Despite global increases in cybersecurity spending, higher education budgets have often adjusted only

for inflation, leaving schools vulnerable. With hackers intensifying their efforts, universities must strengthen cybersecurity measures to mitigate risks (Chin, 2024).

Secondly, educational institutions need to provide security training to their staff and students. Comprehensive security education and training for all personnel is essential for bolstering cybersecurity efforts. Even with a dedicated IT security team, a single mistake by staff, faculty, or students can compromise the entire network. Security training is a cost-effective strategy, particularly for smaller institutions. Integrating brief courses into onboarding processes can cover critical topics such as phishing recognition, VPN setup, safe browsing, strong password practices, and regular system updates. By fostering a culture of cybersecurity awareness through training, schools can significantly reduce the risk of cyber incidents (Chin, 2024).

Lastly, endpoints are among the most accessible entry points for hackers to infiltrate networks, often exploiting human error. Many users overlook basic security practices, inadvertently gently facilitating unauthorized access. While cybersecurity teams monitor network traffic, the sheer number of endpoints—potentially thousands or millions—makes comprehensive coverage challenging. To enhance endpoint security, institutions should deploy solutions such as Endpoint Protection Platforms (EPP), Endpoint Detection and Response (EDR), or Extended Detection and Response (XDR). These tools provide critical functions, including monitoring suspicious activity, issuing real-time security alerts, facilitating remediation, and conducting forensic analysis. Effective implementation of these solutions can significantly improve an institution's ability to detect and respond to threats, strengthening its overall cybersecurity posture (Chin, 2024).

Detection and Response

In the event of a ransomware attack, rapid response is crucial. Effective ransomware detection identifies unusual activity and alerts users, enabling them to halt the spread of the virus before sensitive files are encrypted. Users can isolate affected computers, remove ransomware, and restore systems from secure backups. Early detection is vital for data protection, employing three primary methods: detection by signature, detection by behavior, and detection by abnormal traffic (Baker, 2023).

Detection by signature involves identifying ransomware through unique signatures, such as domain names and IP addresses. This method compares active files against a library of known signatures. While fundamental, this method may struggle to identify new or modified ransomware variants. Detection by behavior monitors unusual activities, such as opening and encrypting numerous files, alerting users to potential threats, and offering protection against other cyberattacks. Detection by abnormal traffic extends behavior-based detection, identifying significant data transfers often associated with sophisticated ransomware attacks that may encrypt and steal data simultaneously, heightening the urgency for effective monitoring (Baker, 2023).

Prompt reaction to any ransomware incident is critical. With the proper monitoring tools, disrupting an attack in progress is often possible. Implementing 24/7 coverage and online detection tools can mitigate damage and expedite system recovery. The following steps are essential during an incident response: determining impacted systems, which involves identifying and isolating affected systems from the network (CONGRESS.GOV, 2021).

If multiple systems are compromised, the network can be taken offline to limit the infection's spread. Powering down equipment is necessary if disconnection is not feasible. However, it should be noted that this may erase volatile evidence. Triage affected systems by prioritizing them based on their criticality to organizational operations. Examining logs allows system logs to be reviewed for indicators of earlier attacks and compromised networks. Determining what happened is essential for establishing how an attack occurred, including the methods used by the perpetrator. Lastly, finding the threat entails determining the ransomware variant and any other malware on the system (CONGRESS.GOV, 2021).

Recovery Strategies

Recovery and restoration following a ransomware attack involve several vital steps. First, organizations should utilize secure backups to restore systems, ensuring that these backups are clean to prevent reinfecting the restored systems during recovery. Implementing lessons learned from the attack is crucial to strengthen security measures, as this helps reduce the likelihood of future incidents. Additionally, deploying ongoing ransomware monitoring solutions is essential for vigilance against potential threats. Finally, completing a post-incident evaluation allows organizations to assess their response and identify areas for improvement, ultimately enhancing their overall cybersecurity posture (CONGRESS.GOV, 2021).

4.2 Government Role

Policy Development

The government plays a crucial role in establishing policies and standards to assist educational institutions in preventing and responding to ransomware attacks. Federal and state governments enact laws and regulations explicitly targeting cybersecurity threats, including ransomware. One significant piece of legislation is the K-12 Cybersecurity Act of 2021, which requires the Cybersecurity and Infrastructure Security Agency (CISA) to study cybersecurity risks specific to K-12 institutions and develop recommendations for cybersecurity guidelines (CONGRESS.GOV, 2021).

In addition to legislation, government agencies develop and promote frameworks and guidelines to help educational institutions prevent and respond to ransomware attacks. The National Institute of Standards and Technology (NIST) provides comprehensive guidelines for ransomware risk management, which can be effectively applied to educational settings (NIST, n.d.). These resources equip institutions with the necessary tools and strategies to enhance their cybersecurity measures and foster a safer learning environment.

Funding and Resources

Governments provide financial support and resources to enhance ransomware defences in educational institutions. Various government agencies offer grants specifically to support cybersecurity initiatives in education, including ransomware prevention. For instance, the Department of Homeland Security's State Homeland Security Program (SHSP) and Urban Area Security Initiative (UASI) grants can be utilized for cybersecurity enhancements in educational institutions (FEMA, 2024)

In addition to financial assistance, government agencies offer technical support and training to help educational institutions prevent and respond to ransomware attacks. The Department of Education's Privacy Technical Assistance Center (PTAC) provides valuable resources on data security best practices, including ransomware prevention strategies (CISA, 2024). This combination of funding and technical assistance empowers educational institutions to bolster their cybersecurity measures and effectively mitigate the risks associated with ransomware attacks.

Collaboration and Information Sharing

Governments facilitate collaboration and information sharing among educational institutions and other stakeholders to enhance ransomware preparedness. They establish platforms for sharing threat intelligence and best practices related to ransomware. For instance, the Cybersecurity and Infrastructure Security Agency (CISA) manages the Federal School Safety Clearinghouse and its corresponding website, SchoolSafety.gov, which offers resources from CISA and other federal agencies to assist schools in preventing, protecting against, mitigating, responding to, and recovering from emergencies. Schools can leverage this information to develop comprehensive security plans and create safe and supportive learning environments (CISA, 2024)

Additionally, governments foster partnerships between educational institutions, private sector companies, and government agencies to address ransomware challenges effectively. One notable example is the K12 Security Information Exchange (K12 SIX), which, although not government-run, works closely with government agencies to share cyber threat intelligence specifically tailored for K-12 schools. This collaboration enhances the overall cybersecurity posture of educational institutions and promotes a unified response to the evolving threat landscape of ransomware attacks (K12SIX, 2024)

Public Awareness Campaign

Governments lead public awareness campaigns to educate the educational community about ransomware threats and prevention. One significant initiative is the ransomware guide published by the Cybersecurity and Infrastructure Security Agency (CISA) in partnership with the Multi-State Information Sharing and Analysis Center (MS-ISAC). This guide includes best practices, and a ransomware response checklist designed to assist educational institutions in preparing for and responding to ransomware incidents. It is actively promoted to schools as part of broader cybersecurity awareness efforts, ensuring that the academic community is equipped with the knowledge and resources necessary to mitigate the risks associated with ransomware attacks (CISA, 2024).

5. Recommendations

This section outlines recommendations to mitigate ransomware risks in educational institutions, focusing on technical measures and educational initiatives. The technical recommendations emphasize the importance of robust network security practices. These practices are crucial for preventing unauthorized access and protecting sensitive data from ransomware attacks. Additionally, the recommendation for all computer users to back up critical data underscores the need for proactive data protection strategies.

5.1 Technical Recommendations

To enhance cybersecurity in educational institutions, it is essential to audit the network for Remote Desktop Protocol (RDP) systems, close unused RDP ports, enforce account lockouts after a specified number of attempts, apply multi-factor authentication (MFA), and log RDP login attempts. Additionally, organizations should update virtual private networks (VPNs), network infrastructure devices, and remote access devices with the latest software patches and security configurations, ensuring that MFA is implemented on all VPN connections to bolster security. In cases where MFA is not feasible, teleworkers must use passwords of 15 or more characters (The Cyber Threat Intelligence (CTI) team, 2024). Furthermore, it is crucial for all computer users—ranging from home users to professional information security officers—to back up their critical data on desktops, laptops, servers, and mobile devices to safeguard against loss or corruption (Heckathorn & Ruggiero, 2012).

5.2 Educational Initiatives

Collaborating with other educational institutions is vital for sharing best practices and lessons learned from ransomware incidents. By engaging in such collaborations, institutions can enhance their cybersecurity resilience and foster a culture of shared knowledge. An excellent example is the Research and Education Networks Information Sharing and Analysis Center (REN-ISAC), which serves over 700 member institutions within the higher education and research community. REN-ISAC promotes cybersecurity operational protections and response strategies, enabling institutions to benefit from the experiences and expertise of their peers (REN-ISAC, 2024). This collaborative approach strengthens individual institutions' defences and contributes to a more secure educational landscape.

6. Conclusion

This paper highlights the critical vulnerabilities government-managed educational institutions face in the face of rising ransomware threats. Key findings include the significant risks associated with Bring Your Own Device (BYOD) policies, as evidenced by case studies like those of the Los Angeles Unified School District and the University of California, San Francisco. These cases illustrate the importance of ethical decision-making during ransomware incidents and the necessity for robust cybersecurity measures, including prioritized spending, security training, and effective detection and response strategies.

Looking ahead, future research should explore ransomware threats and critical information infrastructure (CII) protection across various sectors beyond education. Investigating how different industries adapt to and mitigate similar risks could yield valuable insights and best practices applicable to all sectors. Ongoing government participation is essential for creating flexible laws and resources that address the changing terrain of ransomware attacks. Institutions must proactively bolster their defences and remain attentive as fraudsters become more skilled. Building resilient infrastructures to survive present and future cybersecurity problems requires teamwork and collaboration informed by continuing research and practical experiences.

References

Baker, K. (2023) Crowdstrike. [Online] Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-detection/ [Accessed 20 09 2024].

Brewer, R. (2016) “Ransomware attacks: Detection, prevention and cure”, *Network Security*, 2016, pp. 5–9.

Charandura, K. (2022) SNG Grant Thornton. [Online] Available at: https://www.grantthornton.co.za/Newsroom/cybersecurity-in-the-education-industry/ [Accessed 20 09 2024].

Chen, T.M., Jarvis, L. & McDonald, S. (2024) “Cyberterrorism: Understanding, assessment, and response”, *Springer*.

Chin, K. (2024) Upguard. [Online] Available at: https://www.upguard.com/blog/how-colleges-and-universities-can-prevent-ransomware-attacks [Accessed 20 09 2024].

CISA (2024) [Online] Available at: https://www.cisa.gov/audiences/educational-institutions [Accessed 20 09 2024].

CISA (2024) CISA. [Online] Available at: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/government-services-facilities-sector [Accessed 13 09 2024].

CONGRESS.GOV (2021) Congress. [Online] Available at: https://www.congress.gov/bill/117th-congress/senate-bill/1917 [Accessed 20 09 2024].

Cukier, K.N., Mayer-Schoenberger, V. & Branscomb, L. (2005) "Ensuring (and Insuring?) Critical Information Infrastructure Protection", *SSRN Electronic Journal*.

Department of Education (2022) GOV.UK. [Online] Available at: https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges [Accessed 14 09 2024].

Drishti IAS (2022) Drishti IAS. [Online] Available at: https://www.drishtiias.com/daily-updates/daily-news-analysis/critical-information-infrastructure [Accessed 22 09 2024].

FEMA (2024) FEMA. [Online] Available at: https://www.fema.gov/grants/preparedness/homeland-security [Accessed 20 09 2024].

Grady, A. (2024) Moldstud. [Online] Available at: https://moldstud.com/articles/p-the-impact-of-bring-your-own-device-byod-policies-on-university-it [Accessed 20 09 2024].

Heckathorn, M. & Ruggiero, P. (2012) "Data Backup Options".

Jahankhani, H. et al. (2023) "Ai, Blockchain and self-sovereign identity in Higher Education", *Springer Nature Switzerland*.

Jonathan, L. (2022) NBC. [Online] Available at: https://www.nbclosangeles.com/news/local/lausd-ransomware-attack-stolen-hackers-files-information/2998012/ [Accessed 20 09 2024].

K12SIX (2024) K12SIX. [Online] Available at: https://www.k12six.org/about [Accessed 21 09 2024].

Kapko, M. (2023) NYTimes. [Online] Available at: https://www.cybersecuritydive.com/news/los-angeles-schools-ransomware-health-records/643611/ [Accessed 14 09 2024].

Nico, P. (2013) Prey Project. [Online] Available at: https://preyproject.com/blog/device-security-in-schools-byod-for-lovers-and-haters [Accessed 20 09 2024].

NIST (2024) NIST. [Online] Available at: https://www.nist.gov/ [Accessed 21 09 2024].

O'Gorman, G. & McDonald, G. (2012) "Ransomware: A Growing Menace".

O'Kane, P., Sezer, S. & Carlin, D. (2018) "Evolution of ransomware", *IET Networks*, Volume 7, pp. 321–327.

Pandit, D. (2023) LinkedIn. [Online] Available at: https://www.linkedin.com/pulse/safeguarding-education-vital-importance-cybersecurity/ [Accessed 13 09 2024].

REN-ISAC (2024) REN-ISAC. [Online] Available at: https://www.ren-isac.net/about/index.html [Accessed 20 09 2024].

The Cyber Threat Intelligence (CTI) team (2024) CISecurity. [Online] Available at: https://www.cisecurity.org/insights/blog/renew-your-ransomware-defense-with-cisas-updated-guidance [Accessed 20 09 2024].

Winder, D. (2020) Forbes. [Online] Available at: https://www.forbes.com/sites/daveywinder/2020/06/29/the-university-of-california-pays-1-million-ransom-following-cyber-attack/ [Accessed 14 09 2024].

Zakaria, W.Z., Abdollah, M.F. & Ariffin, A.F. (2017) 'The rise of Ransomware', Proceedings of the 2017 International Conference on Software and e-Business.