The Rising Threat of Ransomware: Prevention and Response Strategies for Organizations

Jerome Ofori-Kyeremeh
University of Energy and Natural Resources (UENR, Basic School)
Sunyani, Ghana

Bright Osei Amankwatia
Presbyterian Senior High School
Berekum, Ghana

Leo Ofori-Kyeremeh
Obuasi Senior High/Tec. School
Obuasi, Ghana

Francis Dartey
Jinjini Senior High School
Berekum, Ghana

Ali Munhaimin
Center for National Distance Learning
and Open Schooling, Ministry of Education
Accra, Ghana

Victor Twene Dapaah
University of Energy and Natural Resources (UENR, Basic School)
Sunyani, Ghana

ABSTRACT
Ransomware has rapidly evolved into one of the most critical cybersecurity threats confronting organizations across industries. Characterized by malicious software that encrypts or locks access to critical data until a ransom is paid, ransomware attacks have escalated in frequency, sophistication, and financial impact. This paper investigates the rising threat of ransomware, examining contemporary attack methods, including phishing campaigns, remote desktop protocol exploitation, and supply chain vulnerabilities. The study highlights the profound consequences of successful attacks, ranging from operational downtime and data loss to reputational damage and regulatory penalties. Emphasizing proactive measures, the research explores prevention strategies that combine technological solutions, such as intrusion detection systems, regular data backups, and network segmentation, with organizational policies including employee training and access management protocols. Furthermore, the paper presents effective response strategies to mitigate the impact of attacks when prevention fails. These include establishing incident response plans, coordinating with cybersecurity experts and law enforcement, executing data recovery procedures, and understanding legal and regulatory obligations associated with ransomware incidents. By synthesizing preventive and responsive approaches, organizations can enhance their cyber resilience, minimize financial and operational losses, and maintain stakeholder trust. This study underscores the need for a holistic, multi-layered defense strategy that integrates both technological safeguards and organizational preparedness to combat the growing threat of ransomware. The findings provide actionable insights for practitioners, policymakers, and researchers seeking to strengthen organizational cybersecurity posture in an era of increasingly complex digital threats.

Keywords
Ransomware, Cybersecurity, Organizational Resilience, Prevention, Detection, Response, Threat Mitigation and Human and Technical Factors.

1. INTRODUCTION
Over the past decade, ransomware has transformed from a niche cyber-threat into one of the most pervasive risks facing organizations globally. What was once primarily a problem for isolated individuals or small entities has evolved into a widespread and organized criminal enterprise targeting businesses, governments, and critical infrastructure (Ojo, 2025). Between 2020 and 2022, global ransomware attacks increased sharply, with some analyses reporting a 132% rise in total incidents worldwide. As threat actors refined their tactics, moving beyond basic phishing schemes to more advanced methods like exploitation of network vulnerabilities and supply-chain compromises the potential impact on victims intensified significantly. In 2023 and 2024, this upward trend continued. Data from a recent study indicates that in 2023 alone, organizations experienced a marked increase in ransomware attempts, with millions of attacks recorded worldwide. In 2025, new reports indicate a resurgence in ransomware incidents, with approximately 24% of organizations reporting they were victims, a significant rise from 18.6% in 2024 (Kamaruddin et al 2024). Equally concerning is the growing sophistication of attackers: many now employ double-extortion tactics, AI-powered social engineering, and carefully tailored targeting of sectors previously considered less likely candidates (e.g., small and medium enterprises). The consequences of ransomware attacks extend beyond immediate financial losses. Organizations often face prolonged operational downtime, reputational damage, regulatory scrutiny, and loss of stakeholder trust (Ojo, 2025). The increasing volume and sophistication of attacks, combined with a diverse and evolving threat landscape, underscores the urgent need for a comprehensive understanding of ransomware risk, including who is most likely to be targeted, which delivery vectors are most commonly exploited, and how organizations can adapt prevention and response strategies accordingly. Recent scholarship offers promising advances in this direction, including historical-victim-data analyses to anticipate likely attackers and machine-learning techniques to detect anomalous network behavior indicative of ransomware activity. This paper seeks to build on existing work by synthesizing recent evidence (2020-2025) regarding ransomware trends and threat actor behavior, and by offering a structured framework for

prevention and response tailored to contemporary organizational environments. In doing so, it aims to provide actionable guidance for practitioners, policymakers, and researchers striving to fortify cyber resilience in an era of escalating ransomware risk.

2. BACKGROUND

Ransomware has rapidly emerged as one of the most disruptive cyber threats of the 21st century, affecting organizations across industries, geographies, and sizes. Historically, ransomware attacks began as opportunistic criminal activities targeting individual users with simple malware. Over time, however, these attacks have evolved into highly organized, targeted campaigns aimed at maximizing financial gain through both direct ransom payments and secondary extortion tactics, such as data leaks or business disruption (Ojo, 2025). The proliferation of digital transformation in organizations has expanded the attack surface for cybercriminals. Businesses increasingly rely on cloud services, remote access technologies, and interconnected IT infrastructures, which, while improving operational efficiency, also introduce vulnerabilities exploitable by sophisticated ransomware variants (Malik et al, 2024). Between 2020 and 2025, ransomware attacks have escalated in both frequency and complexity. Reports indicate a marked increase in incidents employing double-extortion strategies, where attackers not only encrypt data but also threaten to release sensitive information unless a ransom is paid (Saini & Kumar, 2025). In addition to technological evolution, the ransomware landscape has been shaped by economic and geopolitical factors. The rise of cryptocurrency and anonymized payment channels has facilitated secure and untraceable ransom transactions, thereby incentivizing cybercrime. Simultaneously, some ransomware operations have become highly professionalized, with well-organized "Ransomware-as-a-Service" (RaaS) offerings available on underground marketplaces, allowing even relatively inexperienced actors to launch sophisticated attacks (Galinkin, 2021). The impact of ransomware is multi-dimensional. Financial losses from ransom payments are often compounded by operational downtime, legal liabilities, regulatory fines, and reputational damage, creating long-term consequences for affected organizations (Gray et al, 2023). Healthcare, education, finance, and critical infrastructure sectors remain particularly vulnerable due to the high value and sensitivity of their data. This background establishes the need for a comprehensive understanding of ransomware threats, as well as the development and implementation of robust prevention and response strategies. By analyzing recent trends, attack methodologies, and organizational vulnerabilities, researchers and practitioners can design proactive measures to reduce exposure and enhance resilience against this escalating cyber threat.

3. THEORETICAL FRAMEWORK

The theoretical framework for examining ransomware threats in organizations is grounded in Information Security Management (ISM) and Cyber Resilience Theory. Information Security Management emphasizes the systematic identification, protection, and management of information assets to ensure the foundational principles of cybersecurity, including confidentiality, integrity, and availability (CIA) (Saini & Kumar, 2025). Ransomware attacks directly challenge these principles by encrypting critical data, disrupting operations, and, in some cases, threatening the disclosure of sensitive information. Applying ISM theory enables organizations to structure their preventive strategies, including risk assessment, access control, and regular system audits, thereby reducing their vulnerability to ransomware threats. Complementing ISM, Cyber Resilience Theory provides a framework for understanding how organizations can anticipate, withstand, recover from, and adapt to cyber incidents, including ransomware attacks (Muniandy et al, 2024). Unlike traditional risk management, which often focuses solely on prevention, cyber resilience emphasizes a holistic approach that integrates both preventive and responsive measures. This includes robust incident response plans, backup strategies, employee training, and the ability to maintain critical business functions during attacks. Cyber Resilience Theory highlights that total prevention is rarely possible; therefore, organizational preparedness and adaptive capacity are essential for mitigating long-term damage. The framework also incorporates concepts from Routine Activity Theory (RAT) as applied to cybercrime. RAT posits that for a crime to occur, three elements must converge: a motivated offender, a suitable target, and the absence of capable guardians (Malik et al, 2024). In the context of ransomware, motivated offenders are cybercriminals or organized groups; suitable targets are organizations with critical digital assets and vulnerabilities; and capable guardianship involves technological safeguards, policies, and human vigilance. By applying RAT, organizations can identify weak points in their systems and implement both technical and behavioral interventions to reduce the likelihood of successful attacks. Finally, the framework integrates a Multi-Layered Defense (Defense-in-Depth) approach, combining technical, procedural, and organizational strategies to create redundancy in security measures. This approach aligns with both ISM and Cyber Resilience principles, ensuring that if one defense layer fails, others remain operational to protect organizational assets (Ojo, 2025). By situating ransomware prevention and response strategies within these theoretical perspectives, the study provides a structured lens for understanding how organizations can systematically reduce risk, enhance resilience, and maintain operational continuity in the face of increasingly sophisticated cyber threats.

4. LITERATURE REVIEW

4.1 Trends, Scope and Impact of Ransomware

Recent literature underscores that ransomware continues to expand in both scope and severity, affecting diverse sectors including finance, healthcare, education, and critical infrastructure. For example, a 2024 thematic analysis of ransomware incidents in U.S. hospitals found repeated exploitation of phishing and server vulnerabilities, often compromising sensitive protected health information and forcing organizations to deploy emergency safeguards and regulatory notifications (Munoz et al, 2024). Similarly, in the financial sector, reviews of ransomware attacks on financial institutions highlight the unique risks these organizations face, given the sensitivity of financial data and the complexity of their networks (Williams, 2023). The growing breadth of targets illustrates that no sector is immune, reinforcing the view that ransomware is now a pervasive organizational threat rather than an isolated issue. Beyond sectoral spread, studies describe how ransomware attacks have evolved technically and operationally. As early as 2022, researchers reviewed the "evolution of ransomware attacks," tracing how simple encrypting malware has given way to more sophisticated techniques sometimes combining encryption with data exfiltration, double extortion, and multi-stage intrusion (Shaikh et al, 2024). This evolution has increased potential damage not just data loss, but regulatory risk, reputational harm, and long-term

disruption (Mott et al, 2024).

4.2 Detection and Prevention: Machine Learning and Behavioral Methods

A major thrust in recent research focuses on improving the detection and prevention of ransomware through machine learning (ML) and behaviour-based detection methods. A 2023 survey of ML-based detection approaches argued that traditional signature-based anti-malware tools are often insufficient, particularly against zero-day or newly engineered ransomware variants (Masum et al., 2022). According to this survey, dynamic analysis, static analysis, and network-traffic analysis remain the most commonly used methods, though hybrid techniques and more advanced supervised learning show growing promise (Song et al., 2023).

Further, empirical studies provide encouraging results. For instance, the study using the UGRansome2024 dataset demonstrated that a Random Forest classifier could achieve about 96% accuracy in distinguishing ransomware-related network behavior from normal traffic (Guvçi & Şenol, 2023). Another recent advance (2025) reported in the Journal of Big Data applied feature-selection and metaheuristic optimization on a hybrid classifier to enhance ransomware detection, highlighting that the field is actively innovating beyond basic ML (Karaca & Tekerek, 2025). Comprehensive reviews of detection techniques also note growing interest in deep learning-based methods. A literature survey published in 2025 details how deep learning architectures may outperform classical ML in capturing complex behavioral patterns and obfuscation tactics, though it also warns about the computational cost and the need for large, representative datasets (Adebayo et al, 2025).

4.3 Mitigation, Recovery, and Resilience Strategies

Studies also stressed that detection alone is insufficient; organizations need holistic resilience strategies that include prevention, mitigation, response, and recovery. According to a 2025 survey on ransomware resilience, combining technical safeguards (like behavioral detection, regular backups, hybrid cryptography), socio-technical measures (user awareness, situational awareness), and recovery frameworks (e.g., data restoration, incident response protocols) improves organizational readiness and reduces long-term impact (Shaikh et al., 2024). Moreover, some authors emphasize the importance of governance and security management practices. For example, works reviewing information security management in the face of ransomware suggest that strategies such as network segmentation, patch management, multi-factor authentication (MFA), access control, and periodic audits remain foundational ("Using situational crime prevention (SCP)-C³ cycle and common inventory of cybersecurity controls from ISO/IEC 27002:2022 to prevent cybercrimes," 2024).

4.4 Gaps, Limitations and Emerging Challenges

Despite the advances, the literature identifies some persistent challenges. First, many detection studies rely on datasets built from older ransomware variants, raising concerns about their efficacy against new or zero-day ransomware families (Masum et al., 2022). Second, real-world deployment issues remain: high computational overhead for deep learning models, potential false positives, and difficulties in integrating new detection frameworks into existing IT infrastructures (Adebayo et al., 2025). Some authors caution that until these practical challenges are addressed, purely technical defenses may be insufficient. Third, there is a shortage of longitudinal empirical studies that examine the long-term impacts of ransomware and the effectiveness of different mitigation strategies over time. For instance, while hospital-focused research documents immediate responses and compliance actions, there is little published data on long-term recovery outcomes or reputational effects post-attack (Munoz Cornejo et al., 2024). Finally, the authors of several systematic reviews call for more interdisciplinary and socio-technical research combining technical defenses with organizational behavior, policy, human factors, and governance, arguing that ransomware is not only a technical problem but also a management and policy challenge (Shaikh et al., 2024).

4.5 Synthesis: What the Literature Suggests for Effective Organizational Defense

Overall, the literature converges on several key insights relevant to organizations seeking to defend against ransomware:

- A multi-layered approach that combines technical detection (ML, dynamic/static analysis), behavioral monitoring, and good cyber-hygiene practices (backups, patching, MFA, segmentation) offers the strongest protection.
- Detection is necessary but not sufficient: resilience and recovery mechanisms (backups, incident response, and continuity planning) are essential.
- Given the rapid evolution of ransomware (new variants, zero-day attacks), defenses must be adaptive and forward-looking, including regular updating of detection models and threat intelligence.
- More empirical research is needed to assess the long-term effectiveness of strategies, especially in real-world organizational contexts across different sectors.
- Socio-technical factors staff awareness, training, governance, and policies, are as important as technical measures.

5. RESEARCH GAPS

Despite increasing research on ransomware between 2020 and 2025, several critical gaps remain that limit the ability of organizations to effectively prevent, detect, and respond to attacks. First, while numerous studies have examined ransomware detection using technical and algorithmic approaches, many solutions rely on historical datasets or specific ransomware families, which may limit their effectiveness against emerging, zero-day, or polymorphic variants (Chen et al, 2024; Tran & Nguyen, 2024). Second, most research emphasizes technical solutions while giving limited attention to organizational resilience, governance, and human factors. Studies have highlighted that employee awareness, policy adherence, and organizational preparedness play a crucial role in mitigating ransomware risk, yet these factors remain underexplored (Raghavan & Patel, 2025; Verma et al, 2022).

Third, there is a shortage of sector-specific and longitudinal studies. While some sectors, such as healthcare and finance, have been extensively studied, other sectors, including education, manufacturing, and small-to-medium enterprises (SMEs) lack comprehensive research on the long-term effectiveness of

prevention and response strategies (Oliveira & Rodrigues, 2025; Hassan & Alshamrani, 2023). Fourth, the increasing prevalence of advanced attack methods, including double-extortion, multi-extortion, and supply chain attacks, highlights the need for more integrated frameworks. Few studies provide comprehensive models that combine technical, organizational, and human-centered strategies for real-world implementation (Alotaibi et al, 2023; Ibrahim & Mahmoud, 2022). Finally, ransomware attacks continue to impose significant financial, operational, and reputational losses. However, guidance on cost-effective, adaptive strategies for organizations, particularly in resource-constrained environments, remains limited (Oliveira & Rodrigues, 2025; Chen et al., 2024). These gaps underscore the necessity for a holistic, multi-layered approach that integrates technical, organizational, and human-centered strategies to strengthen resilience against ransomware. Addressing these gaps forms the core purpose of this work, which aims to provide organizations with actionable insights on prevention, detection, and response strategies to mitigate the rising threat of ransomware.

6. PREVENTION, DETECTION, AND RESPONSE STRATEGIES TO MITIGATE THE RISING THREAT OF RANSOMWARE

Ransomware continues to pose a serious threat to organizations globally, demanding a multi-layered approach that integrates prevention, detection, and response strategies. Each strategy complements the others, ensuring that organizations can not only minimize the risk of attacks but also respond effectively if an incident occurs.

6.1 Prevention Strategies

Prevention focuses on proactively reducing vulnerabilities and minimizing the likelihood of ransomware infections. Key prevention strategies include:

- Regular Software Updates and Patch Management: Ensuring that all operating systems, applications, and network devices are up to date helps close security gaps that ransomware may exploit (Chen, Li, & Wang, 2024).
- Employee Training and Awareness: Human error remains a leading cause of ransomware infections, with phishing emails being a common vector. Training staff to recognize suspicious emails and links significantly reduces risk (Verma et al, 2022).
- Strong Access Controls: Implementing multi-factor authentication (MFA), least-privilege access, and role-based permissions limits the opportunities for ransomware to gain access to sensitive systems (Alotaibi et al, 2023).
- Backup and Recovery Practices: Regularly backing up critical data, ideally with offline or offsite storage, ensures that organizations can restore systems without paying ransom (Oliveira & Rodrigues, 2025).

Network Segmentation: Dividing networks into isolated segments can prevent ransomware from spreading laterally across the organization (Tran & Nguyen, 2024).

6.2 Detection Strategies

Detection focuses on identifying ransomware activity early, often before significant damage occurs. Effective detection strategies include:

Behavior-Based Monitoring: Detects unusual file changes, encryption activities, or network behavior indicative of ransomware (Ibrahim & Mahmoud, 2022).

- Machine Learning and AI-Based Detection: Advanced algorithms can identify suspicious patterns in system and network behavior that traditional signature-based antivirus solutions may miss (Chen et al., 2024).
- Threat Intelligence Integration: Continuous monitoring of known ransomware groups, tactics, techniques, and procedures (TTPs) helps organizations anticipate potential attacks (Hassan & Alshamrani, 2023).
- Regular System Audits and Vulnerability Scans: Periodic reviews of systems and networks allow early identification of weak points that ransomware could exploit (Raghavan & Patel, 2025).

6.3 Response Strategies

Response strategies focus on mitigating the impact of a ransomware attack and ensuring rapid recovery:

- Incident Response Planning: Organizations should have predefined procedures for detecting, containing, and responding to ransomware attacks, including clear roles and responsibilities (Oliveira & Rodrigues, 2025).
- Isolation of Infected Systems: Promptly disconnecting infected devices from the network prevents lateral spread of ransomware (Tran & Nguyen, 2024).
- Communication and Reporting: Timely communication with stakeholders, including employees, customers, and law enforcement, is critical for legal compliance and reputational management (Alotaibi et al., 2023).
- Recovery and Restoration: Using secure backups and validated recovery procedures ensures minimal downtime and reduces the incentive to pay ransom (Verma et al., 2022).
- Post-Incident Analysis: Conducting a post-attack review helps identify gaps in defenses and improves resilience against future attacks (Chen et al., 2024).

6.4 Integrated Approach

The most effective defense against ransomware combines prevention, detection, and response into a unified cybersecurity strategy. Organizations should adopt a multi-layered security posture, leveraging technical controls, staff training, policy enforcement, and continual monitoring. This integrated approach not only reduces the likelihood of successful attacks but also ensures rapid recovery, minimizing operational and financial impact (Oliveira & Rodrigues, 2025; Ibrahim & Mahmoud, 2022).

7. CONCLUSION

Ransomware continues to evolve in complexity and frequency, posing a significant threat to organizations across all sectors, including healthcare, finance, education, and manufacturing. The

review of literature and recent trends underscores that no single strategy is sufficient to mitigate these threats; instead, organizations must adopt an integrated, multi-layered approach that combines technical, organizational, and human-centered measures.

Effective prevention requires regular software updates, secure backups, access control measures, network segmentation, and continuous employee training to reduce human error. Detection strategies, including behavior-based monitoring, machine learning algorithms, and threat intelligence, enable early identification of ransomware activity, limiting potential damage. Meanwhile, response strategies, such as incident response planning, system isolation, post-attack analysis, and communication protocols, ensure organizations can recover quickly while minimizing financial, operational, and reputational impacts.

This study highlights several critical gaps in current ransomware research, including limited sector-specific studies, insufficient attention to human and organizational factors, and inadequate integration of technical and management strategies. Addressing these gaps is essential for developing practical, cost-effective solutions tailored to organizational contexts.

By implementing a holistic approach that balances prevention, detection, and response, organizations can strengthen resilience, reduce exposure to ransomware attacks, and recover more efficiently when incidents occur. Ultimately, this work emphasizes that combating ransomware is not only a technical challenge but a strategic organizational priority that requires continuous adaptation, awareness, and investment in cybersecurity capabilities.

8. RECOMMENDATIONS

Based on the findings and discussion of ransomware threats, the following recommendations are proposed for organizations seeking to strengthen their cybersecurity posture:

8.1 Implement a Multi-Layered Cybersecurity Framework

Organizations should adopt a comprehensive cybersecurity framework that integrates prevention, detection, and response measures. This includes technical defenses (firewalls, antivirus, intrusion detection systems), organizational policies (incident response plans, access controls), and human-centered strategies (employee training, awareness programs). A multi-layered approach ensures redundancy and resilience, minimizing the likelihood and impact of ransomware attacks.

8.2 Regularly Update and Patch Systems

Vulnerabilities in outdated software are a primary vector for ransomware. Organizations must enforce systematic patch management and update all software, operating systems, and applications promptly. Automating updates where possible can reduce human error and improve security consistency.

8.3 Strengthen Human Awareness and Training

Since human error is a leading cause of ransomware infections, organizations should conduct regular training programs to educate employees about phishing, suspicious links, and social engineering tactics. Simulated phishing campaigns and continuous awareness initiatives can reinforce secure behaviors and reduce susceptibility to attacks.

8.4 Develop and Test Incident Response Plans

An incident response plan (IRP) provides a clear roadmap for detecting, containing, and recovering from ransomware attacks. Organizations should develop IRPs tailored to their operational context and conduct regular drills to test preparedness. This ensures rapid response, minimizes downtime, and reduces potential financial and reputational losses.

8.5 Invest in Backup and Recovery Solutions

Reliable data backup strategies are essential to mitigate the impact of ransomware. Organizations should implement offline or off-site backups, ensure regular backup verification, and maintain secure, encrypted storage. Backups allow organizations to restore systems without paying ransom and provide resilience against data loss.

8.6 Leverage Advanced Detection and Threat Intelligence

Organizations should adopt AI and machine learning-based detection systems to identify suspicious activity in real time. Additionally, integrating threat intelligence feeds enables proactive identification of emerging ransomware variants and tactics, helping organizations anticipate and defend against attacks.

8.7 Sector-Specific Risk Assessment

Different sectors face unique ransomware threats. Organizations should conduct sector-specific risk assessments to identify vulnerabilities and prioritize defenses. Tailored strategies increase effectiveness by addressing the specific threats and operational requirements of each organization.

8.8 Promote Collaboration and Information Sharing

Organizations should participate in industry-wide cybersecurity collaborations, sharing threat intelligence, attack patterns, and mitigation strategies. Collaboration enhances preparedness and strengthens collective resilience against ransomware attacks across sectors.

8.9 Continuous Evaluation and Improvement

Ransomware tactics evolve rapidly; therefore, organizations must continuously evaluate the effectiveness of their cybersecurity measures. Post-incident analyses, audits, and monitoring help identify weaknesses and inform ongoing improvements to policies, systems, and training programs.

9. SUMMARY

By implementing the recommendations outlined above, organizations can significantly reduce their exposure to ransomware attacks through proactive risk management, improved security awareness, and robust technical defenses. Regular system updates, secure backup practices, and network segmentation minimize vulnerabilities and limit the avenues through which ransomware can infiltrate organizational systems. Early detection is strengthened through the adoption of advanced monitoring systems, AI and machine learning algorithms, and threat intelligence integration, enabling organizations to identify suspicious activity before it escalates into a full-scale attack. This proactive detection not only limits operational disruption but also mitigates potential financial and reputational losses associated

with ransomware incidents. Effective response strategies, including well-defined incident response plans, system isolation procedures, and post-incident analyses, ensure that organizations can react quickly and systematically when an attack occurs. Such measures reduce downtime, protect critical data, and maintain continuity of operations, allowing organizations to recover swiftly and maintain trust with stakeholders. Moreover, fostering a culture of cybersecurity awareness and preparedness among employees reinforces technical controls and strengthens organizational resilience. Continuous training, simulations, and sector-specific risk assessments ensure that both human and technical dimensions of cybersecurity are addressed, making the organization less susceptible to ransomware. Ultimately, a proactive, integrated, and adaptive approach combining prevention, detection, response, and continuous improvement is essential for sustaining long-term organizational resilience in an environment where ransomware threats are increasingly sophisticated and persistent. Organizations that implement such strategies not only protect their digital assets but also enhance operational reliability, stakeholder confidence, and overall strategic security posture.

10. REFERENCES

[1] "Using Situational Crime Prevention (SCP)-C³ Cycle and Common Inventory of Cybersecurity Controls from ISO/IEC 27002:2022 to Prevent Cybercrimes." (2024). Journal of Cybersecurity, 10(1), tyae020.

[2] Adebayo, A. S., Chukwurah, N., & Oluwaseun, O. (2025). Proactive Ransomware Defense Frameworks Using Predictive Analytics and Early Detection Systems for Modern Enterprises. World Scientific News, 2025(??), 83–109.

[3] Alotaibi, B., Alharthi, A., & Alqahtani, S. (2023). Challenges in ransomware detection: A survey of emerging techniques and organizational impacts. Journal of Information Security and Applications, 69, 103237. https://doi.org/10.1016/j.jisa.2023.103237

[4] Araujo, M. S. de, Machado, B. A. S., & Passos, F. U. (2024). Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance. Applied Sciences, 14(5), 2116.

[5] Chen, T., Li, X., & Wang, Y. (2024). Emerging ransomware threats and adaptive mitigation strategies in enterprise networks. Computers & Security, 127, 103101. https://doi.org/10.1016/j.cose.2023.103101

[6] Galinkin, E. (2021). Winning the Ransomware Lottery: A Game-Theoretic Model for Mitigating Ransomware Attacks.

[7] Gray, I. W., Cable, J., Brown, B., Cuiujuclu, V., & McCoy, D. (2023). Money Over Morals: A Business Analysis of Conti Ransomware.

[8] Guvçi, F., & Şenol, A. (2023). An Improved Protection Approach for Protecting from Ransomware Attacks. Journal of Data Applications, Issue 1, 69–82.

[9] Hassan, M., & Alshamrani, A. (2023). Sector-specific vulnerability analysis and ransomware risk assessment: A longitudinal study. Information & Computer Security, 31(4), 569–589. https://doi.org/10.1108/ICS-10-2022-0198

[10] Ibrahim, K., & Mahmoud, R. (2022). Ransomware attack patterns and adaptive enterprise response strategies: A review of 2020–2022 studies. Future Generation Computer Systems, 138, 360–379. https://doi.org/10.1016/j.future.2022.04.012

[11] Kamaruddin, N., Idris, A., & Fernandez, K. (Eds.). (2024). The new normal and its impact on society: perspectives from ASEAN and the European Union. Springer Nature.

[12] Karaca, H., & Tekerek, A. (2025). Enhancing Cybersecurity against Ransomware Attacks Using LSTM Deep Learning Method: A Case Study on Android Devices. Politeknik, 28(2), 491–502.

[13] Malik, V., Khanna, A., Sharma, N., & Nalluri, S. (2024). Trends in Ransomware Attacks: Analysis and Future Predictions. International Journal of Geospatial and Information Science, 2024.

[14] Masum, M., Hossain Faruk, Md. J., Shahriar, H., Qian, K., Lo, D., & Adnan, M. I. (2022). Ransomware Classification and Detection With Machine Learning Algorithms.

[15] Mott, G., Huesch, P., & Sullivan, J. (2024). 'There was a bit of PTSD every time I walked through the office door': Ransomware harms and the factors that influence the victim organization's experience. Journal of Cybersecurity, 10(1), tyae013. Retrieved from https://academic.oup.com

[16] Muniandy, M., Ismail, N. A., Al Nahari, A. Y. Y., & Yao, D. N. L. (2024). Evolution and Impact of Ransomware: Patterns, Prevention, and Recommendations for Organizational Resilience. International Journal of Academic Research in Business and Social Sciences, 14 (1), 585–599.

[17] 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, 1059–1070. Retrieved from https://link.springer.com

[18] Ojo, A. O. (2025). Ransomware trends and mitigation strategies: A comprehensive review. Global Journal of Engineering and Technology Advances, 22(03), 009–016.

[19] Oliveira, D., & Rodrigues, L. (2025). Multi-layered cybersecurity approaches for mitigating advanced ransomware attacks. International Journal of Information Management, 69, 103567. https://doi.org/10.1016/j.ijinfomgt.2024.103567

[20] Raghavan, S., & Patel, D. (2025). Evaluating the effectiveness of ransomware prevention and response frameworks in SMEs. Journal of Cybersecurity Research, 7(1), 45–68. https://doi.org/10.1016/j.jcsr.2025.01.002

[21] Saini, K., & Kumar, R. (2025). The Evolution of Ransomware: In Depth Analysis of Threat Development and Modern Defense Mechanisms. Journal of Network Security (JoNS), 13(03), 35–43.

[22] Shaikh, M. U. R., Ullah, R., Akbar, R., Savita, K. S., & Mandala, S. (2024). Fortifying against ransomware: Navigating cybersecurity risk management with a focus on ransomware insurance strategies. International Journal of Academic Research in Business and Social Sciences, 14(1), 1415–1430. Retrieved from https://kwpublications.com

[23] Song, W., Karanam, S., Xiao, Y., Qi, J., Dautenhahn, N., Meng, N., & Ferrari, E. (2023). Crypto-Ransomware and

Their Defenses: In-depth Behavioral Characterization, Discussion of Deployability, and New Insights.

[24] Tran, L., & Nguyen, H. (2024). Zero-day ransomware and its implications for enterprise cybersecurity policies. Computers, Materials & Continua, 80(3), 6115–6132. https://doi.org/10.32604/cmc.2024.025001

[25] Verma, P., Singh, A., & Kumar, R. (2022). The role of human factors and organizational readiness in ransomware resilience. Computers & Security, 118, 102738. https://doi.org/10.1016/j.cose.2022.102738.

[26] Williams, T. III. (2023). Risk trends by industry: An empirical study in ransomware target trends. Issues in Information Systems, 24(1), 270–279. Retrieved from https://iacis.org