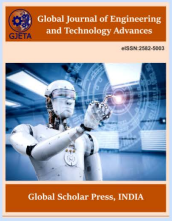
Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/



(REVIEW ARTICLE)

Check for updates

Ransomware trends and mitigation strategies: A comprehensive review

Ojo, Abraham Olasunkanmi *

Publicis Sapient, Houston, TX 77002, United States of America.

Global Journal of Engineering and Technology Advances, 2025, 22(03), 009-016

Publication history: Received on 09 January 2025; revised on 24 February 2025; accepted on 27 February 2025

Article DOI: https://doi.org/10.30574/gjeta.2025.22.3.0038

Abstract

Ransomware has emerged as one of the most pervasive and damaging cybersecurity threats, targeting organizations across industries with increasing frequency and sophistication. This malicious software encrypts critical data, rendering it inaccessible until a ransom is paid, often causing significant operational disruptions and financial losses. Over time, ransomware tactics have evolved, incorporating advanced encryption methods, double extortion strategies, and the exploitation of emerging technologies to maximize impact. These developments have amplified the challenge for organizations striving to defend against such attacks. This paper explores the dynamic landscape of ransomware, highlighting the latest trends in attacker methodologies and their implications for cybersecurity. Key findings reveal that a multi-layered approach to mitigation encompassing robust endpoint protection, timely data backups, employee training, and proactive threat intelligence is critical for minimizing risks. Additionally, this work identifies emerging areas for future research, including the integration of artificial intelligence in threat detection and the development of international policies to combat cyber extortion. By understanding the evolving threat and adopting comprehensive defense strategies, organizations can better safeguard their operations and resilience against ransomware attacks.

Keywords: Ransomware Attacks; Multi-Layered Approach; Cyber Extortion; Mitigation Strategies

1. Introduction

Ransomware is a type of malicious software designed to block access to a computer system or encrypt critical data until a ransom is paid, and this cybersecurity threat has gained notoriety due to its devastating impact on individuals, businesses, and public institutions [3]. The rise in remote work, digitization, and reliance on interconnected systems has further amplified its prevalence, making it a critical issue in the cybersecurity domain, and unlike traditional malware, ransomware often incorporates psychological manipulation to compel victims to comply with demands [22]. As organizations increasingly rely on digital infrastructure, the potential for disruption caused by ransomware grows, threatening financial stability, reputation, and operational continuity [3]. The evolution of ransomware can be traced back to the late 1980s, with the introduction of the "AIDS Trojan," which demanded payment via postal mail [3]. Over the years, ransomware has advanced significantly in terms of technology and tactics, and in the mid-2000s, the advent of stronger encryption algorithms allowed attackers to create more effective and irreversible encryptions, leading to the rise of crypto ransomware [29]. Recent years have witnessed the emergence of double and triple extortion techniques, where attackers not only encrypt data but also threaten to release sensitive information or disrupt operations unless payment is made. These sophisticated strategies, combined with the use of ransomware-as-a-service (RaaS) platforms, have lowered the barrier to entry for cybercriminals, further escalating the threat landscape [16]. Given the increasing frequency and severity of attacks, adequate understanding of the trends and evolution of ransomware is essential for developing effective mitigation strategies, and this also highlight the need for a proactive approach to cybersecurity [4]. Awareness of current tactics, such as targeted attacks on critical infrastructure and supply chain vulnerabilities enables organizations to prioritize defenses and allocate resources efficiently. Additionally, comprehending attacker motivations and methodologies helps in designing robust response frameworks that minimize

* Corresponding author: Abraham Olasunkanmi

Copyright © 2025 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Liscense 4.0.

downtime and financial impact [26, 4]. By staying ahead of emerging trends, organizations can enhance their resilience and protect sensitive data against evolving threats. Therefore, this review aims to provide an overview of ransomware as a critical cybersecurity threat, by exploring its historical evolution, and current trends. Specifically, the objectives of this review are threefold. First, the review aims to analyze the latest advancements in ransomware tactics and their implications for organizations, identify and evaluate mitigation strategies, including technological, procedural, and policy-based approaches, as well as propose future directions for research and collaboration in combating ransomware attacks.

1.1. Brief Review of Literature: The Ransomware Ecosystem

The anatomy of a ransomware attack typically unfolds in three main stages or phases: infection, encryption, and ransom demand. The infection phase exploits vulnerabilities in systems or relies on social engineering techniques, such as phishing emails, malicious links, or compromised software updates, to gain unauthorized access, and once inside, the ransomware encrypts critical files using robust algorithms, rendering them inaccessible to the victim, and finally, attackers deliver a ransom note, often providing instructions on how to pay the ransom [21], typically in cryptocurrency, to regain access to the encrypted data. This process is designed to exert maximum pressure on the victim to comply.

Considering the evolution of ransomware, the early ransomware, such as CryptoLocker, emerged in the early 2010s and marked a turning point in the sophistication of cyber extortion, and this utilized strong encryption and demanded payments in Bitcoin, making it challenging to trace transactions, which primarily spread through email attachments and exploited unpatched systems, causing widespread disruption and financial losses [22]. Then, the modern ransomware campaigns and Ransomware-as-a-Service (RaaS) have evolved to incorporate advanced tactics, such as double extortion, where attackers threaten to leak stolen data in addition to encrypting it [17]. Raas platforms have further revolutionized the ecosystem by providing pre-packaged ransomware tools to affiliates in exchange for a share of the profits [22]. This model has lowered the technical barrier for entry, enabling even novice attackers to participate in ransomware campaigns and significantly increasing the volume and sophistication of attacks and the common monetization methods is cryptocurrency payments. According to Hampton and Baig (2015), cryptocurrency has become the preferred medium for ransom payments due to its perceived anonymity and ease of transfer. Attackers often use mixing services and decentralized exchanges to obscure the origin of funds, complicating efforts to trace transactions. Additionally, some ransomware groups have established partnerships with underground money laundering networks, further enhancing their ability to evade detection and enforcement actions [29].

1.2. Ransomware Families and Case Studies

There are many family members associated with ransomware. Parts of the key families include, “WannaCry”, which is a ransomware worm that emerged in 2017, exploited a vulnerability in the Windows operating system [6], and this infected over 200,000 systems across 150 countries, causing widespread disruption, particularly in the healthcare sector. Therefore, WannaCry highlighted the critical importance of timely patch management and global collaboration in addressing ransomware threats. Another one, known as “Ryuk” is a targeted ransomware variant known for its focus on high-value organizations, and it often combines with other malware, such as TrickBot, to infiltrate networks and maximize impact [21]. Ryuk has been linked to multimillion-dollar ransom demands, emphasizing the financial motivations driving these campaigns. Besides this, Jimmy (2023) also stressed about a ransomware named “REvil”, and this is also known as Sodinokibi. REvil is a RaaS platform responsible for numerous high-profile attacks, including incidents targeting supply chains and critical infrastructure. Its operators have employed sophisticated techniques, such as data exfiltration and double extortion, to increase their leverage over victims. REvil’s activities underscore the need for coordinated efforts to disrupt ransomware groups and mitigate their impact.

1.3. Trends and Impact of Ransomware Attacks

Modern ransomware campaigns have adopted double extortion tactics, where attackers not only encrypt victims’ data but also exfiltrate sensitive information, and it is regarded as an increased sophistication and double extortion and data leaks tactics [30] However, if the ransom is not paid, the attackers threaten to publish the stolen data on dark web forums or leak it to competitors, which significantly increasing the pressure on victims, and such act leverages both financial and reputational risks to maximize compliance [7]. Further, recent ransomware attacks have increasingly targeted critical infrastructure and supply chains, recognizing their strategic importance and vulnerability. The Colonial Pipeline attack in 2021 exemplified this trend, causing widespread fuel shortages and prompting a federal response. Such incidents underscore the far-reaching impact of ransomware on national security and public safety [24, 29].

The rise of RaaS platforms and democratization of ransomware is another trend [21]. The proliferation of RaaS platforms has lowered the barriers to entry for cybercriminals, democratizing ransomware attacks [43]. Aspiring

attackers can now purchase or lease sophisticated ransomware tools, enabling them to execute high-impact campaigns without advanced technical expertise. This commoditization has led to a significant increase in the frequency and scale of attacks globally.

Ransomware operators are now increasingly tailoring their campaigns to specific sector, industries and geographic regions. This signifies a sector, geographic and industry-specific targeting trends [36, 28]. For instance, healthcare, education, and financial sectors remain prime targets due to the high value of their data and the critical nature of their operations [18, 19, 22]. Geographically, attackers often focus on regions with weaker cybersecurity measures or higher ransom payment potential, such as North America and Europe. Another common trend is the use of social engineering and exploitation of zero-day vulnerabilities, and this remains a cornerstone of ransomware attacks, with phishing emails and fraudulent websites being common infection vectors [12]. Additionally, attackers are increasingly exploiting zero-day vulnerabilities to gain unauthorized access to systems before patches are available [21]. These methods highlight the importance of both user awareness and timely vulnerability management in preventing ransomware incidents.

In terms of impact, ransomware attacks impose substantial economic costs on the affected individuals and/or organizations. Direct financial losses include ransom payments, which often range from thousands to millions of dollars, while recovery expenses encompass costs associated with forensic investigations, data recovery efforts, system restoration, and implementation of enhanced security measures [23]. Additionally, operational downtime caused by inaccessible systems can lead to lost revenue, supply chain disruptions, and reduced productivity [27]. For small and medium-sized enterprises (SMEs), these financial burdens can be particularly devastating, potentially leading to business closures. There is also a societal impact of ransomware which extends beyond economic losses to include severe disruptions to critical services. For instance, attacks on healthcare systems, such as the 2017 WannaCry incident, have resulted in delayed medical treatments and jeopardized patient safety and security [6]. Similarly, ransomware targeting energy infrastructure, exemplified by the Colonial Pipeline attack, has caused fuel shortages and economic ripple effects [24, 29], and all these attacks hinder essential services and undermining public trust.

Organizations affected by ransomware attacks may equally face significant legal and regulatory repercussions [35, 37]. Data protection laws, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), impose strict requirements for safeguarding personal data. Failure to comply can result in substantial fines and legal actions, while organizations may be held liable for breaches that expose customer or employee information [14, 37]. The increasing regulatory focus on cybersecurity underscores the importance of robust incident response plans and proactive compliance measures. In addition, the psychological toll on victims and organizational morale cannot be underestimated. This psychological impact of ransomware attacks on both individuals and organizations is profound, such that the victims often experience stress, anxiety, and feelings of violation due to the loss of sensitive data and operational disruptions [39]. For employees, according to Solove and Citron (2018), as well as Alzahrani et al. (2019), the aftermath of an attack can lead to diminished morale, fear of job insecurity, and frustration over compromised systems, while organizational leadership may equally face reputational damage and public scrutiny, further exacerbating the emotional toll. Addressing these psychological effects requires transparent communication, employee support programs, and a strong emphasis on fostering resilience within the workforce.

1.4. Mitigation Strategies against Ransomware Attack

There are many mitigation measures put in place against ransomware attacks. First is the proactive measures, such as employee training and awareness programs because one of the most effective defenses against ransomware is educating employees on recognizing and responding to potential threats [22]. Regular training sessions can improve awareness of phishing tactics, safe browsing habits, and best practices for handling suspicious emails and links. Another proactive strategy is regular system patching and vulnerability management by keeping software and systems up to date is crucial in mitigating the risk of ransomware. According to Malik et al. (2024), regular patching ensures that known vulnerabilities are addressed, reducing opportunities for attackers to exploit outdated systems. Similarly, implementation of robust endpoint detection and response (EDR) tools is another vital proactive measure because EDR tools provide real-time monitoring and detection of malicious activities on endpoints [38, 32]. These tools can identify ransomware behaviors, isolate affected systems, and prevent the spread of infection across networks.

There are also preventive measures, such as multi-factor authentication (MFA). Implementation of MFA technologies adds an additional layer of security, requiring users to verify their identities through multiple methods; an approach which significantly reduces the risk of unauthorized access to sensitive systems and accounts [34, 11]. Besides, segmenting networks into smaller, isolated sections has been reported to limits the spread of ransomware within an organization, a practice known as network segmentation and least-privilege access controls [40]. Enforcing least-

privilege access ensures that users and applications only have access to the resources necessary for their roles, reducing the potential attack surface. Besides, developing and testing ransomware-specific incident response plans is a good strategy that enables organizations to develop comprehensive incident response plans, tailored to ransomware attacks because this ensures preparedness and identifies areas for improvement [28]. Another preventive measure is maintaining secure and redundant backups [31]. Data backup and recovery strategies is a critical aspect of ransomware resilience and regularly backing up data to both on-site and cloud-based systems ensures that organizations can restore operations without paying a ransom, while testing backup integrity and recovery processes is equally important to ensure reliability during an actual incident [10, 31].

1.5. Legal and Ethical Considerations

In terms of negotiating with attackers versus refusing to pay ransoms, organizations face a difficult ethical dilemma when confronted with ransom demands. Paying ransoms can incentivize further attacks, while refusing to pay may result in data loss or public exposure. Each decision should be informed by legal, operational, and ethical considerations [35, 13]. Collaborating with law enforcement and cybersecurity experts can help organizations navigate the aftermath of an attack [42]. These entities provide valuable support in investigating incidents, recovering data, and mitigating future risks. In fact, law enforcement involvement can also contribute to the broader effort to dismantle ransomware networks and prosecute offenders.

2. Role of Policy and Regulations in Combating Ransomware

Ransomware attacks continue to be a major threat to global cybersecurity, and effective responses to mitigate their impact rely heavily on robust policy and regulatory frameworks. Various international and national efforts aim to counter these attacks, as well as legal obligations to ensure consumer protection. First and foremost, international collaboration is essential to tackle ransomware due to the borderless nature of cybercrime [29]. A notable example of international effort is the Budapest Convention on Cybercrime, formally known as the Convention on Cybercrime of the Council of Europe. The Budapest Convention, adopted in 2001, is the first international treaty designed to address crimes committed via the internet and other computer networks [33]. It facilitates cooperation between member states in investigating and prosecuting cybercrime, including ransomware attacks. The Convention focuses on the process for extraditing cybercriminals across borders, making it easier for law enforcement to hold offenders accountable, the treaty enhances mutual legal assistance between countries in terms of gathering evidence and conducting joint investigations, and provides a legal framework for the criminalization of activities such as unauthorized access to systems, data interference, and the distribution of malicious software, which are often associated with ransomware attacks [33]. In addition to the Budapest Convention, other global efforts such as the G7 and G20 Cybersecurity Working Groups and the Global Forum on Cyber Expertise (GFCE) facilitate information-sharing and cooperation between countries to develop strategies to combat ransomware and other cyber threats [41, 15].

Similarly, the European Union's EU Cybersecurity Strategy for the Digital Decade (2020) outlines efforts to strengthen cybersecurity across the region, including improving resilience to cyberattacks such as ransomware [5]. The strategy promotes the development of EU-wide cybersecurity standards**,** cooperation between member states, and improved capacity for responding to ransomware incidents. Countries like the U.S. and other developed nations also leverage frameworks like the NIST Cybersecurity Framework**,** which helps organizations identify and manage cybersecurity risks, including those related to ransomware [5]. These frameworks provide guidelines for organizations to assess their current cybersecurity posture and implement safeguards against cyber threats. These national strategies typically exemplify the importance of cyber hygiene practices**,** incident response plans, and resilience measures to mitigate the impact of ransomware.

2.1. Role of Cyber Insurance in Ransomware Mitigation

Cyber insurance is increasingly viewed as an essential tool in mitigating the financial impact of ransomware attacks, and it also serves as a safety net for organizations that may not have the resources to absorb the full financial impact of a ransomware attack, while it equally also plays a role in incentivizing organizations to adopt stronger cybersecurity measures to reduce the likelihood of such an attack [22]. These insurance policies typically cover all the costs (for instance, ransom payments, incident response costs, and business interruption costs) associated with responding to an attack [25]. Ransom payments policies may cover the cost of paying the ransom, although this practice is discouraged by law enforcement agencies, while **i**ncident response costs coverage can include the expenses for forensic investigations, legal fees, and crisis communication efforts. The **b**usiness interruption costs related to cyber insurance can indeed compensate for lost revenue due to downtime caused by a ransomware attack [20].

In response to the growing frequency of ransomware attacks, the cyber insurance industry has also begun implementing stricter requirements for policyholders, such as mandatory security measures, and exclusion of ransom payments. In term of the **m**andatory cybersecurity measures, insurers often require businesses to implement basic cybersecurity measures, such as multi-factor authentication, regular backups, and employee training to qualify for coverage, while in the case of **e**xclusion of ransom payments, some insurers are now excluding ransom payments from coverage or imposing higher premiums for those that seek reimbursement for ransom payments [25]. This discourages the practice of paying ransoms, while at the same time aligns with law enforcement's advice not to fund criminal activity.

3. Legal Obligations for Reporting Ransomware Incidents and Protecting Consumer Data

Legal frameworks governing the reporting of ransomware incidents and the protection of consumer data are crucial in holding organizations accountable and protecting public trust. Many countries have laws that require organizations to report cybersecurity incidents, including ransomware attacks, to relevant authorities. For example, the European Union's General Data Protection Regulation **(**GDPR) imposes strict data protection obligations on organizations, including the requirement to notify data protection authorities within 72 hours of discovering a data breach, which may include ransomware attacks involving consumer data [14]. GDPR also requires organizations to implement appropriate technical and organizational measures to ensure data security, which includes protecting against ransomware.

In the U.S., many states have data breach notification laws that require businesses to inform consumers when their personal information has been compromised, including in the case of a ransomware attack. These laws **(**U.S. Data Breach Notification) are intended to ensure that affected individuals can take steps to protect themselves from potential identity theft or fraud. In the same vein, **t**he U.S. Cybersecurity Information Sharing Act (CISA) (2015) also encourages private entities to share cybersecurity threat information, including ransomware-related threats, with the U.S. government. The act aims to improve the national defense against cyber threats by ensuring that private organizations have a clear path for reporting incidents to federal agencies, while the legal obligations also include requirements for protecting consumer data [28]. For example, companies that fall victim to ransomware attacks may be subject to regulatory scrutiny and fines if they have not taken adequate steps to secure data under laws like the GDPR or the California Consumer Privacy Act (CCPA)**.** These regulations promote transparency, accountability, and consumer protection, ensuring that organizations take proactive measures to secure data and report incidents promptly to mitigate harm to affected individuals [29, 28].

Future direction: Encouraging collaboration, enforcing accountability, and supporting organizational preparedness can significantly assist in the fight against ransomware. These efforts collectively contribute to strengthening the global response to ransomware and other cyber threats. More importantly, the future of AI and ML in cybersecurity is marked by continued innovation and integration with other technologies. The emerging trends discussed above, including federated learning, explainable AI, AI-powered threat hunting, and the evolution of collaborative intelligence, suggest a future where AI-driven cybersecurity solutions are not only more effective but also more adaptable, transparent, and aligned with privacy and regulatory requirements. As these technologies continue to evolve, they will play a pivotal role in combating the increasingly sophisticated cyber threats of today and tomorrow.

4. Conclusion

As ransomware continues to evolve in both sophistication and frequency, it poses an ever-growing threat to organizations across the globe. The rise of advanced attack techniques, such as double extortion, the targeting of critical infrastructure, and the exploitation of vulnerabilities in supply chains, has made ransomware one of the most pervasive and financially damaging cyber threats. Organizations, regardless of size or sector, are increasingly vulnerable to these attacks, which can result in substantial financial losses, reputational damage, and the exposure of sensitive data. The implications for businesses are far-reaching, affecting not only their operational continuity but also customer trust and compliance with regulatory requirements. Therefore, the fight against ransomware requires coordinated efforts at the international, national, and organizational levels. Policies and regulations such as the Budapest Convention, national cybersecurity frameworks, cyber insurance practices, and legal obligations for reporting ransomware incidents and protecting consumer data play a critical role in mitigating the impact of ransomware. The future of ransomware defense depends on how quickly organizations, governments, and researchers can adapt to emerging threats and harness the power of innovative technologies. This is to say that embracing a multi-layered defense approach, investing in collaborative cybersecurity efforts, and fostering research and development, individuals and organizations can significantly reduce the risks posed by ransomware and improve the resilience of our digital infrastructures. As the landscape continues to evolve, a unified and proactive approach will be key to overcoming the ever-present challenge of ransomware.

Compliance with ethical standards

Funding

This research received no funding from any source.

Disclosure of conflict of interest

The author declared no conflict of interest.

Ethical Considerations

This study was carried out in line with the Helsinki's declaration on research guidelines, which are: "anonymity, informed consent, privacy, confidentiality, and professionalism".

References

[1] Adapa, V.R.K (2024). Zero Trust Architecture Implementation in Critical Infrastructure: A Framework for Resilient Enterprise Security. International Journal of Advanced Research in Engineering and Technology (IJARET), 15(6), 76–89.

[2] Alzahrani, A., Alshahrani, H., Alshehri, A., & Fu, H. (2019). An intelligent behavior-based ransomware detection system for android platform. In 2019 1st IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA'19). IEEE, 28–35.

[3] Bellamkonda, S. (2017). Cybersecurity and Ransomware: Threats, Impact, and Mitigation Strategies. Journal of Computational Analysis and Applications, 23(8), 1424-1429.

[4] Bello. A., & Maurushat, A. (2020). Technical and behavioural training and awareness solutions for mitigating ransomware attacks. In Computer Science On-line Conference. Springer, 164-176.

[5] Bendiek, A., & Kettemann, M.C. (2021). Revisiting the EU Cybersecurity Strategy: A Call for EU Cyber Diplomacy. SWP Comment, No.16, February 2021. Available at: https://www.swp-berlin.org/publications/products/comments/2021C16_EUCyberDiplomacy.pdf

[6] Chen, Q., & Bridges, R.A. (2017). Automated behavioral analysis of malware: A case study of wannacry ransomware. In 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA'17). IEEE, 454–460.

[7] Conti, M., Gangwal, A., & Ruj, S. (2018). On the economic significance of ransomware campaigns: A Bitcoin transactions perspective. Computers & Security 79 (2018), 162–189.

[8] Cybersecurity Information Sharing Act (CISA) (2015). CISA Act of 2015, S. 754, 114th Congress.

[9] Elete, T.V. (2024). Impact of ransomware on industrial control systems in the oil and gas sector: Security challenges and strategic mitigations. Computer Science & IT Research Journal, 5(12), 2664-2681. https://doi.org/10.51594/csitrj.v5i12.1759

[10] Elisan, C. (2015). Advanced Malware Analysis. New York, NY, USA: McGraw-Hill Education.

[11] Fernandez, E.B., & Brazhuk, A. (2024). A critical analysis of Zero Trust Architecture (ZTA). Computer Standards & Interfaces, 89, 103832. https://doi.org/10.1016/j.csi.2024.103832

[12] Gallegos-Segovia, P.L., Bravo-Torres, J.F., Larios-Rosillo, V.M., Vintimilla-Tapia, P.E., Yuquilima-Albarado, I.F., & Jara-Saltos, J.D. (2017). Social engineering as an attack vector for ransomware. In 2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON'17). IEEE, 1-6.

[13] Gawazah, L., Rondla, A., & Balhareth, M.S.A. (2024). To Pay or Not to Pay: The US Colonial Pipeline Ransomware Attack. Available at: https://www.researchgate.net/publication/383206534_To_Pay_or_Not_to_Pay-_The_US_Colonial_Pipeline_Ransomware_Attack

[14] General Data Protection Regulation (GDPR), (2016). "General Data Protection Regulation," European Union, Brussels, Belgium, Regulation 2016/679.

[15] Greco, E., & Marconi, F. (2024). Technological Innovation Cybersecurity: The Role of the G7. The Istituto Affari Internazionali (IAI) Commentaries. May, 2024. Available at: https://www.iai.it/sites/default/files/iaicom2422.pdf

[16] Gudimetla, S. (2015). Beyond the Barrier - Advanced Strategies for Firewall Implementation and Management. NeuroQuantology, 13(4), 558-565. https://doi.org/10.48047/nq.2015.13.4.876.

[17] Hampton, N., & Baig, Z.A. (2015). Ransomware: Emergence of the Cyber-Extortion Menace. In Proceedings of the 13th Australian Information Security Management Conference, Perth, Australia, 30 November–2. pp. 47–56.

[18] Hathaliya, J.J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. Comput. Commun., 153, 311–335.

[19] Hathaliya, J.J., Tanwar, S., Tyagi, S., & Kumar, N. (2019). Securing electronics healthcare records in Healthcare 4.0: A biometric-based approach. Comput. Electr. Eng., 76, 398–410.

[20] Huang, K., Siegel, M., & Madnick, S. (2017). "Cybercrime-as-a-Service: Identifying Control Points to Disrupt." MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, Cambridge, MA, USA, Working Paper CISL# 2017-17, 2017.

[21] Jimmy, FNU (2023). Understanding Ramsomeware Attacks: Trends and Prevention Strategies. Journal of Knowledge Learning and Science Technology, 2(1), 180-209. https://doi.org/10.60087/jklst.vol2.n1.p214

[22] Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I.E. (2022). Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions. Sustainability, 14, 8. https://doi.org/10.3390/su14010008

[23] Kharraz, A. Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). Cutting the Gordian knot: A look under the hood of ransomware attacks. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Springer, 3-24.

[24] Kilovaty, I. (2023). Cybersecuring the Pipeline. Houston Law Review, 60(3), 605-651.

[25] Laszka, A., Johnson, B., Grossklags, J., & Felegyhazi, M. (2017). "On the Economics of Ransomware," in Proc. Int. Conf. Decision and Game Theory for Security, Vienna, Austria, 2017, pp. 397-417.

[26] Luo, X., & Liao, Q. (2007). Awareness education as the key to ransomware prevention. Information Systems Security 16, 4, 195-202.

[27] Maimo, F.L., Huertas, C.A., Perales G.A.L., Garcia, C.F.J., Weimer, J., & Lee, I. (2019). Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. Sensors, 19, 1114.

[28] Malik, V., Khanna, A. Sharma S,N., & Nalluri, S. (2024). Trends in Ransomware Attacks: Analysis and Future Predictions. International Journal of Global Innovative and Solutions. https://doi.org/10.21428/e90189c8.f2996624

[29] McIntosh, T., Kayes, A.S.M., Chen, Y.P., Ng, A., & Watters, P. (2021). Ransomware Mitigation in the Modern Era: A Comprehensive Review, Research Challenges, and Future Directions. ACM Comput. Surv., 54(9), Article 197. https://doi.org/10.1145/3479393

[30] Mercaldo, F., Nardone, V., & Santone, A. (2016). "Ransomware Inside Out," in Proc. 2016 11th Int. Conf. Availability, Reliability Security (ARES), Salzburg, 2016, pp. 628-637.

[31] Min, D., Park, D., Ahn, J., Walker, R., Lee, J. Park, S., & Kim, Y. (2018). Amoeba: An autonomous backup and recovery SSD for ransomware attack defense. IEEE Computer Architecture Letters 17, 2, 245–248.

[32] National Institute of Standards and Technology (NIST), (2013). "Guide to Enterprise Patch Management Technologies," National Institute of Standards and Technology, Gaithersburg, MD, USA, Special Publication 800-40 Rev. 3, 2013.

[33] Nguyen, C.L., & Golman, W. (2020). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'. Computer Law & Security Review, 40, 105521, https://doi.org/10.1016/j.clsr.2020.105521

[34] Pookandy, J. (2021). Multi-factor authentication and identity management in cloud CRM with best practices for strengthening access controls. International Journal of Information Technology and Management Information Systems (IJITMIS), 12(1), 85-96.

[35] Rapuzzi, R., & Repetto, M. (2018). Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model. Future Gener. Comput. Syst., 85, 235-249.

[36] Richardson, R., & North, M.M. (2017). Ransomware: Evolution, mitigation and prevention. Int. Manag. Rev., 13, 10.

[37] Romsom, E. (2022). Countering global oil theft: Responses and solutions: WIDER Working Paper.

[38] Sikorski, M., & Honig, A. (2012). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. San Francisco, CA, USA: No Starch Press, 2012.

[39] Solove, D.J., & Citron, D.K. (2018). Risk and Anxiety: A Theory of Data-Breach Harms. Texas Law Review, 96, 737-786, 2018.

[40] Sun, N., Zhang, J., Rimba, P., Gao, S., Zhang, L.Y., & Xiang, Y. (2019). "Data-Driven Cybersecurity Incident Prediction: A Survey." IEEE Communications Surveys & Tutorials, 21 (2), 1744-1772.

[41] World Economic Forum (WEF), (2023). The G20 Digital Agenda: Cross-Presidency Priorities. White Paper. Available at: https://www3.weforum.org/docs/The_G20_Digital_Agenda_2023.pdf

[42] Yuri, B., & Jeroen, S. (2022). Zero Trust Validation: From Practical Approaches to Theory, Scientific Journal of Research and Reviews, https://doi.org/10.33552/SJRR.2020.02.000546

[43] Cimpanu, C. (2020). "Ransomware gangs are now cold-calling victims if they restore from backups without paying," ZDNet, Dec. 2020. [Online]. Available at: https://www.zdnet.com/article/ransomware-gangs-are-nowcold-calling-victims-if-they-restore-from-backups-without-paying/