International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 12
***Article Received:** 25 July 2022 **Revised:** 12 September 2022 **Accepted:** 30 November 2022*

Ransomware Prevention and Mitigation Strategies

Sandeep Reddy Gudimetla
Consultant, HCL America., Dallas, Tx.

Abstract: The past few decades have seen a rise in internet use and digital transformations in organizations. Digital platforms have been fully integrated into daily life activities. Nonetheless, cybercriminals have taken advantage of internet overreliance, by devising different forms of cyberattacks. Ransomware is one of the common types of cyberattacks. In this research, a systematic literature review was conducted to examine different effective strategies for preventing and mitigating ransomware attacks. Twenty-four articles were sourced from databases like PubMed, ScienceDirect, and ACM Digital Library and reviewed. The analysis revealed five key themes; ransomware detection methods, user awareness and training, access and control measures, data backup strategies, and the implementation of security policies. Based on these themes, it was evident that organizations could safeguard their systems and networks from ransomware attacks through measures like using data backup, enforcing access control measures, ensuring employee awareness of security threats, and enforcing robust security policies.

keywords: *Ransomware Prevention, Mitigation Strategies*

Background of study

Over the past three decades, the world has experienced increased internet connectivity and digitalization. However, the increased use and reliance on the internet has enabled cybercriminals to create and launch different kinds of cyberattacks, both small-scale and large-scale. These attacks have targeted corporations and individuals globally (Alansari et al., 2019). Cybersecurity criminals have relied on the internet, communication platforms, and information channels to cyberattack. One of the most common types of cyberattacks is ransomware. According to Alshaikh et al. (2020), there has been an exponential rise in ransomware attacks over the past decade. A ransomware attacks are a form of cybersecurity where attackers access, steal, and lock computer data or functionalities and extort money from victims before releasing the data back or unlocking the blocked functionalities. Threat actors have developed different mechanisms to deploy ransomware attacks without detection. In most cases, the attackers use malicious advertisements, emails, and drive-by downloads to trick unsuspecting users into allowing access to their critical data or computer systems. There are three categories of ransomware attacks: crypto, locker, and scareware (Beaman et al., 2021). In scareware, attackers usually target victims by using pop-up ads to trick them into presuming that they need to download a particular software, where they use coercion techniques to download malware into the targeted devices. In this type of ransomware, threat actors exploit the fear instead of encrypting the data or locking the device. Usually, scareware attacks do not result in any harm to the victim's device. The goal of attackers in locker ransomware is to block key computer functions (Beaman et al., 2021). When this ransomware is deployed, attackers encrypt particular files that lock the keyboard or computer screen. However, the issue can quickly be addressed by running an on-demand virus or rebooting the device in a safe mode. Also, with locker ransomware, limited user access to the affected computer device can be allowed. Crypto ransomware is the most dangerous and likely unreversible. The technique deploys encryption techniques like RSA and AES; these two techniques cannot be reversed when implemented during ransomware attacks. Ransomware dates back to the 1980s. The first-ever cyber extortion threat occurred in 1989 when the PC Cyborg Trojan targeted a computer. According to Wade (2021) the virus encrypted all files on the computer's C drive and hid directories, rendering the system unusable. During the 1990s and the early 2000s, ransomware attacks became more common. However, they were conducted mainly by hobbyist hackers who sought notoriety through cyber vandalism and pranks. Today, ransomware has become a significant business strategy for cybercriminals. Initially, threats targeted individuals; however, today, corporations have become key targets of ransomware attacks. Some of the sectors that attackers commonly target include healthcare, transportation, government institutions, and financial and banking industries. Also, the number of ransomware attacks has rapidly increased because it has become much easier to obtain ransomware-as-a-service and other ransomware toolkits, giving threat actors more opportunities to execute their attacks.

One major cyberattack event that brought to light the potential impact of ransomware attacks was the WannaCry and Petya attacks, which occurred in May 2017 (Mansfield-Devine, 2017). This cyberattack affected over thirty thousand machines across one hundred and fifty countries within the first three days after launch (Mansfield-Devine, 2017). Numerous organizations across sectors, such as healthcare, education, and even the oil and gas industry, were affected; millions of money were lost. In each attack, the cybercriminals demanded between 300 and 600 USD to release decryption keys to the affected organizations. Also, during the COVID-19 period, the number of cyberattacks increased drastically. More companies began to adopt remote-working options, shifting the workplace paradigms to home-based working scenarios (Saleous et al., 2022). As a result, security controls weakened, giving attackers more opportunities to trick unsuspecting individuals using COVID-19-themed phishing emails. On numerous occasions, phishing campaigns disguised as crucial messages related to the pandemic prompted users to click certain links. Users were tricked into obtaining sensitive information about the shortage of surgical masks and the COVID-19 vaccine and reporting back to work messages; also, the pandemic resulted in higher levels of unemployment, as most companies had to lay off some of their staff due to economic downturns (Saleous et al., 2022). Hence, more people were inspired to engage in cybercrimes like ransomware to earn a living. In this study, a systematic review will be conducted to examine the countermeasures and preventing strategies for mitigating ransomware attacks.

Research problem

Ransomware attacks usually result in substantial financial losses, decreased productivity, disruption of regular business activities, and damage to the reputations of the affected individuals or organizations (Connolly et al., 2020). The State of Ransomware 2021' by Sophos revealed that the average cost for organizations to recover from a ransomware attack was US$1.85 million (Adam, 2021). The costs included aspects like expenses related to downtime, networks, lost opportunities, personnel, devices, and ransom payments. Notably, this amount is nearly double the US$761,106 cost documented in 2020 (Adam, 2021). Furthermore, these attacks can potentially lead to an irreversible loss of data or files. There is no assurance that paying the ransom will release the locked system or files. According to Connolly et al. (2020), organizations that pay the ransom have an average cost twice as high for recovering from the attack. Connolly et al. (2020) add that it is projected that ransomware assaults will incur a global cost of $20 billion by the end of 2021, a significant increase from $325 million in 2015. According to Chigada & Madzinga (2021), the COVID-19 epidemic resulted in a series of destructive attacks, which targeted healthcare organizations, vaccine research labs, and contact tracing apps. Based on the presented figures, it is evident that to successfully identify and reduce the impact of future attacks, there is a need to understand the patterns and characteristics of ransomware and its different forms. Emerging ransomware versions, driven by their profitability, are constantly evading existing antivirus software and other detection measures. Therefore, it is crucial to determine the most effective strategies that can be deployed to mitigate ransomware attacks. More research needs to be conducted to determine effective strategies for detecting and preventing ransomware attacks. This study will conduct a systematic literature review to examine the prevention and mitigation strategies for ransomware attacks.

Research questions

a) What are the best technological measures that enterprises may take to protect themselves from ransomware attacks?
b) To what extent can enterprises reduce the possibility of ransomware attacks by training and using awareness programs for employees, and how can these programs be effectively implemented?
c) How can companies successfully employ policies, legislation, and governance in the fight against ransomware attacks?

Literature review

Strategies for preventing and mitigating ransomware attacks

Some of the best methods for protecting enterprises against ransomware attacks were investigated by Beaman et al. (2021). Strict access control, data backup, user knowledge of ransomware assaults, and key management are some of the examples, according to the report. The AntiBotics solution was developed by Ami et al. (2018) and has three primary components: a driver for enforcing policies, an interface for defining policies, and a system for challenges and responses. This application protects data from accidental loss or tampering by combining biometric authentication (like fingerprint recognition) with human response (like CAPTCHA). In order to establish access control, AntiBotics routinely identifies problems. The program's ability to authorize executable objects is based on a rule set by the administrator and the results of errors that occur while trying to change or remove files (Ami et al., 2018). The fact that Windows is the only OS that has been evaluated is a downside of this application. In addition, current ransomware cannot evade AntiBotics, but future ransomware could be able to change to avoid it. Ransomware, for instance, may bypass AntiBotics by tucking itself inside a legitimate process and staying there until it is permitted (Ami et al., 2018). Also, ransomware might attempt to disguise itself by changing the

***Article Received:** 25 July 2022 **Revised:** 12 September 2022 **Accepted:** 30 November 2022*

name of a protected directory. Nevertheless, AntiBotics can hinder this by creating an obstacle during the renaming process. Genç et al. (2018) created an access control method based on the understanding that ransomware, when lacking access to genuine randomness, depends on the fake or pseudo-random number generators modern operating systems provide to produce keys for its operations. The suggested technique aims to reduce ransomware attacks by recognizing the false generators of random numbers functions as crucial assets, regulating access to their APIs, and preventing unauthorized applications from using them (Genç et al., 2018). Their technique underwent testing with 524 operational ransomware samples and successfully thwarted 94% of them, including prominent variants such as NotPetya, WannaCry, CryptoLocker, Locky, and CryptoWall. One more effective approach to combat ransomware is to back up data (Alshaikh et al., 2020; Beaman et al., 2021). Ransomware attacks can be mitigated by periodically backing up data stored on computers or networks, according to Beaman et al. (2021). The damage, however, will only affect data created after the last backup. It is important to carefully decide on the frequency and retention time of backups because backing up large amounts of data can be expensive. A number of scholars have put forth different methods for backing up data. Thomas and Galligher (2018) looked at ransomware in depth, several paradigms for functional backup design, and how well backups protected against ransomware. They went on to say that information security risk assessments should be better and that ransomware should be a particular focus. In addition, they unveiled a new method for assessing backup systems in the context of risk assessments for information security. By allowing auditors to do comprehensive analyses of backup systems, this technology improves an organization's ability to protect itself from and recover from ransomware attacks. Min et al. published Amoeba in 2018; it is an autonomous solid-state drive (SSD) with backup and recovery capabilities that can withstand ransomware attacks. A dedicated hardware accelerator is included into the Amoeba system to quickly detect web page ransomware threats (Min et al., 2018). In addition, it uses an accurate backup control approach to reduce the amount of space needed to store backups of the original content. The authors included Amoeba to the Microsoft SSD emulator so they could test their system. According to Min et al. (2018), they tested the ransomware by analyzing real block-level traces taken while the program was running. In comparison to the cutting-edge solid-state drive (SSD) FlashGuard, Amoeba outperformed it in terms of performance and space efficiency, and it showed no extra costs during testing. Key management is another effective technique, which encompasses recovering the encryption key deployed to encrypt data and files by attackers and using it to decrypt the locked data without paying the ransom (Beaman et al., 2021). Nonetheless, this technique is more significant when preventing specific ransomware samples, mainly those that directly complex code the key into their practicable binary. This approach may be less practical in hybrid ransomware models because the key is only available in plaintext when actively encrypting files (Beaman et al., 2021). Different critical management approaches can be deployed to mitigate ransomware attacks. Certain ransomware programs employ a symmetric session key to carry out encryption. The key is saved in the victim's computer, which encrypts the user's files. Kolodenker et al. (2017) created a key backup system called Paybreak, dependent on signatures. PayBreak employs a critical escrow methodology wherein session keys, including the symmetric key utilized by the attacker, are securely stored in a vault. During the testing process, PayBreak effectively retrieved all files that had been encrypted using recognized encryption signatures. The security of the symmetric encryption key is crucial for producers of ransomware. Moreover, a significant portion of ransomware solely uses AES to encrypt data. Taking this into consideration, Bajpai and Enbody (2020) devised a side-channel assault on the critical management of ransomware to retrieve ransomware keys that are exposed in the system's memory while the encryption process is underway. Their attack exploits the fact that the encryption method is visible on the host system, irrespective of the specific cryptographic API being used or whether a cryptographic API is utilized at all (Bajpai & Enbody, 2020). In initial trials, their attack successfully detected vulnerable AES keys in the memory of ransomware processes, achieving a 100% success rate. This included identifying such keys in versions of NotPetya, WannaCry, LockCrypt, CryptoRoger, and AutoIT. Other authors have also examined how user awareness and training can help reduce incidences of ransomware attacks in organizations. According to Chung, (2019), using measures that empower employees to safeguard themselves against ransomware attacks is integral in organizations. This is particularly crucial because, as previously said, ransomware attacks are progressively focusing on institutions such as banking or healthcare businesses. The authors provided a list of five preventive measures that employees should adhere to: Installing anti-malware or anti-virus software on all computers and mobile devices in use, using unique and strong passwords for both personal and work accounts, regularly backing up files to external hard drives, and avoiding clicking on suspicious files or email attachments (Chung, 2019). Additionally, mirror shielding technology like NeuShield can serve as an additional failsafe strategy for data protection. Thomas

(2018) investigated strategies for users and staff to prevent ransomware attacks. However, the main focus of the study was on methods for individuals to avoid falling victim to phishing attempts, which often serve as the initial stage of ransomware attacks. The author surveyed many security specialists and put forward various recommendations based on the survey results. One suggestion was to categorize firm employees according to their knowledge of phishing and the significance of their roles (Thomas, 2018). Following the segmentation process, the subsequent suggestion was to create specialized training programs for each group. This training should incorporate practical illustrations emphasizing the severity and harm caused by phishing, utilize authentic case studies, and encompass genuine occurrences within the firm. By sharing genuine and personal experiences, individuals will gain a profound understanding of the harmful consequences of spear phishing and be prompted to take more personal measures to protect themselves.

The significance of employee training and awareness programs in minimizing the likelihood of ransomware attacks

The significance of providing cybersecurity awareness training to employees in business cannot be exaggerated. In an era where cyber threats are becoming increasingly advanced and widespread, firms must provide their employees with the required knowledge and abilities to recognize and address possible cyber hazards. Luo and Liao (2007) assert that although corporations allocate substantial money to advanced cybersecurity tools and technology, relying on these measures is insufficient to guarantee comprehensive protection against cyber threats. Employees are generally perceived as the most vulnerable point in the security system, as they may mistakenly become victims of social engineering techniques, open harmful email attachments, or unintentionally reveal confidential information (Luo & Liao, 2007). Therefore, enterprises must emphasize cybersecurity awareness training as a core element of their overall cybersecurity strategy. Cybersecurity awareness training offers advantages beyond preventing data breaches and assaults. An educated and attentive workforce can cultivate a culture of cybersecurity awareness within the firm. Employees with a comprehensive understanding of the potential hazards and optimal methods are more inclined to make better judgments while dealing with confidential data and utilizing corporate systems, networks and devices (Luo & Liao, 2007). Consequently, this decreases security events, thereby avoiding potential financial losses, legal obligations, and reputational harm.

Beaman et al. (2021) also examined the significance of training users in mitigating ransomware attacks in organizations. According to the study, many cyberattacks are linked to vulnerabilities caused by organisational human actors (Beaman et al., 2021). For instance, the Volkswagen attack occurred due to data in an inadequately protected file, whereas the attack on Colonial Pipeline was attributed to using a recycled password (Bajpai et al., 2020). The impacts of human activities, or lack thereof, can cause significant harm, such as decreased productivity, financial losses, and damage to credibility and reputation (Nobles, 2018). Furthermore, the repercussions are frequently not immediately evident. This has a detrimental effect on the level of urgency that employees attribute to cybersecurity. According to Kapoor et al. (2021), training end-users is one potential approach to enhance cybersecurity. The emphasis on end-user behaviour is attractive because several cybersecurity problems currently encountered in organizations cannot be resolved entirely by technology alone. Kapoor et al. (2021) add that defensive mechanisms like firewalls, antivirus software, and spam filters can mitigate certain attacks, but other dangers often emerge and result in catastrophic results. Furthermore, implementing technical measures may not always be feasible when considering the specific duties that employees and other end-users are required to carry out. Although employees are typically cognizant of the security risks they may encounter, they must also fulfil their job responsibilities promptly. Shadow security behaviours are employed to adhere to job requirements and security standards to the greatest extent possible (Sillic, 2019). Shadow security is when employees cannot adhere to their organisation's security policies and methods. Sillic (2019) states that, as a result, employees tend to seek out and utilize alternative technologies or solutions that their organisation has not approved. This implies that when individuals find imposed norms and restrictions unattractive, they seek ways to bypass them. This also emphasizes that end-user conduct is essential in averting cyberattacks linked to human behaviours. A practical approach is to train end-users regarding the many hazards organizations and institutions encounter. Beaman et al. (2021) explored different training approaches that corporations can rely to address the human causes of cybersecurity issues. The study reveals that when seeking to enhance end-users' cybersecurity practices, the primary emphasis should be placed on awareness campaigns to communicate cybersecurity concerns effectively (Beaman et al., 2021). According to van Steen et al. (2020), who analysed nineteen federal cybersecurity awareness programs, all of the materials employed in these efforts were similar. Information was solely disseminated through 'campaign stationery' such as posters or bookmarks and websites that occasionally featured video content. The dissemination of information through text-based modalities is widely favoured in these campaigns because of its inherent advantages of being more convenient, expeditious, and cost-effective compared to alternative approaches.

Methodology

Research design

This study adopted a systematic literature review as the research methodology, where existing literature on the common prevention and mitigation strategies for ransomware attacks was analyzed. Systematic reviews are integral research methodologies because they facilitate a thorough and deep analysis of relevant literature sources to answer research questions (Watson & Webster, 2020). In this current study, the review follows a meticulous plan, where details have been divided into different sources. The first section outlines the search strategy (how literature was sourced) the inclusion and exclusion criteria, and the subsequent sections contain details of the analysis.

Search strategy

The search process in this current study entailed using a rigorous and methodical approach to collect, examine and synthesize existing literature on the research subject. The goal was to comprehensively determine relevant studies from academic databases, grey literature sources, and conference papers. The first step entailed choosing the keywords and search terminologies related to the research topic. The keywords adopted in this case were “ransomware,” “mitigation strategies,” “ransomware prevention,” and “data protection.” In the search, Boolean operators “AND,” “OR,” and “NOT” were deployed to combine the keywords effectively. For example, the search process included: “ransomware AND prevention AND mitigation” OR ransomware AND cybersecurity.

The above search approach was deployed to gather sources from critical academic databases: ScienceDirect, ACM Digital Library, IEEE Xplore, and PubMed. Sourcing the papers from more databases ensured broad coverage. Additionally, grey literature sources, for example, government publications and reports from cybersecurity organizations, were also considered sources of relevant literature.

Inclusion and exclusion criteria

Inclusion and exclusion criteria were applied to source articles most relevant to the research topic. Studies that met inclusion criteria, such as those published in less than five years, relevant to ransomware prevention and mitigation strategies, published in English and published in reputable academic sources, such as peer-reviewed journals and dissertations, were considered. The exclusion criteria entailed removing studies covering irrelevant topics (for example, addressing other types of cyberattacks), duplicate studies, non-English publications, and articles not available in full text. The initial database search yielded 463 articles. Among them, 152 were sourced from ScienceDirect, 76 from PubMed, 87 from IEEE Xplore, and 148 from ACM Digital Library. An additional 23 articles were sourced from grey literature, making the total number of searched articles 486. Titles and abstracts were screened, and articles not related to ransomware (97), duplicate articles (63), and articles older than ten years (39) were excluded. The remaining articles (264) were further scrutinized for eligibility. The goal was to select full-text articles only. Articles that did not focus on ransomware prevention and mitigation (161) covered irrelevant content (46) and were published in other languages besides English were eliminated (33). From the screening, 24 articles were left for review.

Table 1: Inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
Studies focusing on ransomware attacks, prevention, mitigation strategies, or related topics within the realm of cybersecurity.	Studies not directly related to ransomware, cybersecurity, prevention, or mitigation
Peer-reviewed journal articles, conference papers, theses, dissertations, and reputable reports from cybersecurity organizations	Non-academic materials, websites, blogs
Studies published in not more than ten years	Studies older than ten years
Studies published in English	Papers not available in English
Studies discussing strategies, technologies, best practices, or frameworks specifically aimed at preventing ransomware attacks or mitigating their impact.	Duplicate studies

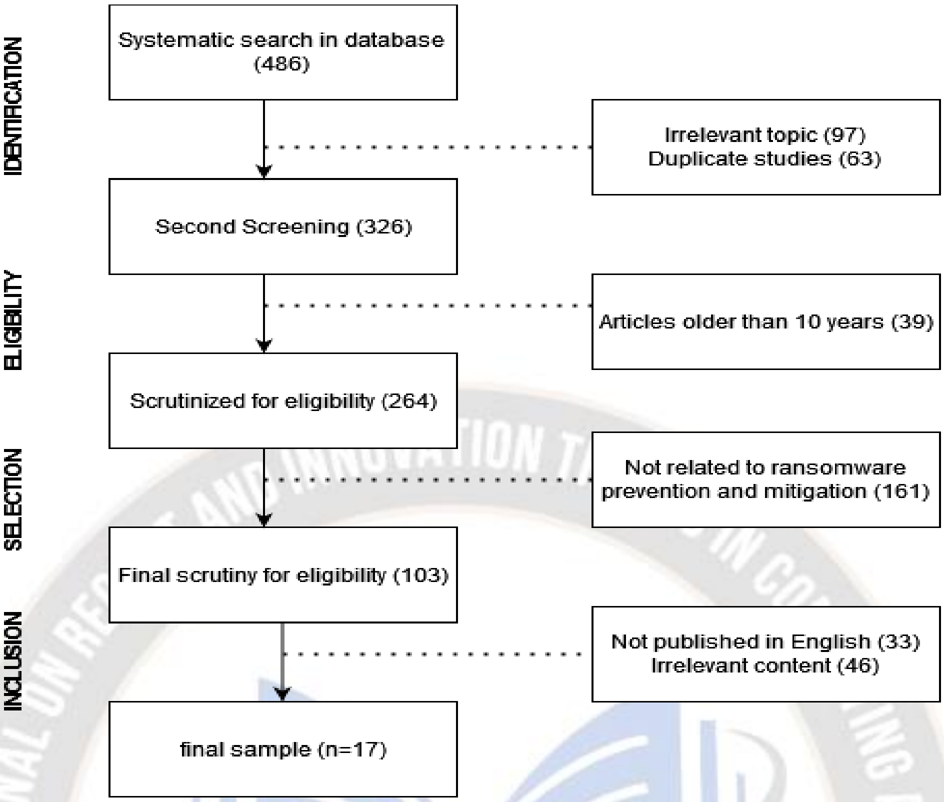
IDENTIFICATION
ELIGIBILITY
SELECTION
INCLUSION
Systematic search in database (486)
Irrelevant topic (97)
Duplicate studies (63)
Second Screening (326)
Articles older than 10 years (39)
Scrutinized for eligibility (264)
Not related to ransomware prevention and mitigation (161)
Final scrutiny for eligibility (103)
Not published in English (33)
Irrelevant content (46)
final sample (n=17)

Fig 1: Prisma diagram

Initial findings

The key themes that emerged from the review included the following key aspects: ransomware detection methods and prevention and mitigation. Since the focus of this study, prevention and mitigation strategies were analyzed further by breaking them into specific prevention techniques. The table below shows how the number of papers that addressed each theme:

Table 2: Key identified themes

Theme	**Number of articles covered**
Ransomware detection methods	3
Data backup strategies	5
User awareness and training	5
Access control measures	3
Implementing security policies	3

Ransomware detection methods

Detection methods offer preemptive alerts to prompt the user to respond promptly before an attack occurs. These approaches depend on ransomware assaults that expose the actions of the attack on devices and systems, for example, the file system or the network system. Cabaj and Mazurczyk (2016) introduced a technique that utilizes Software-Defined-Networking (SDN) for detecting ransomware assaults by monitoring their activities. By closely examining the network connection between the CryptoWall and Locky ransomware families, researchers could identify the presence of ransomware by analyzing the patterns of HTTP messages and their corresponding content sizes (Cabaj & Mazurczyk, 2016). In order to find a detection method that works on both Android and Windows, Monika et al. (2016) studied several ransomware families on both platforms. The researchers came to the conclusion that in order to detect Android malware, it is crucial to monitor permission requests that occur during software downloads. Finding and detecting suspicious file system activity is an important part of the detection procedure in a Windows environment (Monika et al., 2016). To develop a highly effective method of ransomware detection, researchers need to examine the many traits displayed by this type of malware. Following these steps will teach consumers how to protect themselves from ransomware.

Preventive and mitigation strategies

Cybersecurity professionals have been on the lookout for reliable ways to protect businesses' data from ransomware as it has been on the increase. Businesses hit by ransomware need to take precautions to lessen the effect of the assault. On the other hand, it is crucial for people think about ways to stop attacks before they even happen. Ransomware prevention involves taking proactive measures to prevent an attack, whereas ransomware mitigation involves reacting to an assault to minimize the harm inflicted. The literature synthesis conducted in this current study identified various principles and guidelines to combat ransomware attacks. The examined journal articles created a comprehensive set of guidelines for preventing and mitigating ransomware. Although these are not perfect solutions, following these suggestions can help prevent and reduce the impact of ransomware attacks. All computer users can examine the guidelines; however, some are particularly relevant to business users.

Data backup strategies

Organizations must possess crisis resilience to effectively respond to disasters by implementing contingency plans for data recovery. Several studies highlight the importance of periodically creating computer data backups to mitigate the impact of an attack (Huang et al., 2017; Kharraz & Kirda, 2017; Thomas & Galligher, 2018). (Thomas and Galligher (2018) elucidate the significance of data backups to resist ransomware. Users should periodically generate a duplicate of their computer data, ensuring that these duplicates are marked with a timestamp. Consequently, once data has been restored, a company can be assured that it will be readily accessible. Specialist programs exist explicitly designed to create data backups; they include external storage devices such as USB flash drives, cloud storage solutions like Dropbox, rewritable optical discs, or backup tapes (Manjezi & Botha, 2019). Nevertheless, ensuring that data is stored offline is crucial, as ransomware can infiltrate data backup systems (Erridge, 2016). Consequently, it is crucial to ensure that backup storage is not linked to the internet. Additionally, backups should be performed daily to guarantee the retrieval of up-to-date information. Typically, data backup is a method of mitigating risk. When a company is impacted by ransomware, this strategy makes retrieving the data from backup files possible. Backup storage serves as a secure refuge for data that a company relies on regularly, ensuring that business operations may continue without interruption in case of a ransomware attack.

Cybersecurity awareness creation and training

As discussed in the paper, human behaviour has a significant role in promoting or obstructing cyber security. Kapoor et al. (2021) assert that, it is crucial to offer users with training on how to proactively identify and effectively handle ransomware assaults. Ransomware criminals often utilize social engineering techniques by employing phishing emails to deliver their malicious payload (Pope, 2016). Thus, organizations should implement cyber security awareness campaigns to enlighten users about the perils of ransomware attacks and effective strategies for prevention and mitigation (Pope, 2016). Training and education can empower employees knowledgeable about cybercrimes to assess, identify, and address vulnerabilities (Chung, 2019; Tiu & Zolkipli, 2021). By training new and existing personnel, organizations will create a cyber-security culture that will have significant advantages in the present and future (Chung, 2019). Tiu & Zolkipli (2021) express that cybersecurity programs should prioritize enlightening users about phishing emails, as they are the primary carriers of ransomware. Cybersecurity education is a proactive approach to equipping people with the necessary information and skills to recognize and avoid ransomware threats. If all personnel possess awareness regarding this infection, firms can avoid incurring financial losses resulting from ransomware attacks.

Implementing access control measures

Access control is a vital aspect of online security. Regarding ransomware, it might not be the definitive resolution to preventing attacks. Nevertheless, implementing access restrictions based on organizational responsibilities can be an effective mitigation approach ((McIntosh et al., 2021; Parkinson, 2017). According to Parkinson (2017), access control makes it challenging for attackers to obtain valuable data after attacking a regular user via phishing emails and ransomware based on the user's credentials. Hence, in case of a ransomware attack, the implementation of access control measures can effectively thwart any further exploitation of computer data by unauthorized entities.

Implementing security policies

According to Mishra et al. (2022), companies must establish security policies to safeguard the business by implementing various security policies or regulation. These regulations should provide safeguards for companies against cybercrimes, specifically ransomware attacks. According to Manjezi and Botha (2019), businesses must create and uphold effective rules for employees who do not comply with the regulations. Savaş & Karataş (2022) add that a mere compilation of optimal methodologies and regulations may not be entirely effective; they must be accompanied by active implementation. Policies should be formulated to effectively safeguard enterprises from ransomware attacks, focusing on prevention and mitigation strategies. For instance, a backup strategy policy will outline specific guidelines for implementing backup measures and identify the most suitable backup techniques for the firm. Additional policies will prioritize password management and access control functionalities.

Discussion and conclusion

The modern world is information-centric. Valuable and private data is mostly kept in digital format. As a result, criminal organizations have striven to acquire this information to gain financial benefits unlawfully. Cybercrimes, such as ransomware attacks, have severely impacted major corporations by subjecting them to cyber extortion. Ransomware has undergone significant advancements in the past few years, making it among the most renowned and perilous cyber-attack forms. Researchers and cyber-security specialists have been working to discover a universal remedy for this cyber-attack. Various research activities have resulted in the creation of detection methodologies and the identification of ransomware assault strategies. Several techniques for preventing and mitigating ransomware attacks have also been investigated. This current study conducted a systematic literature review to examine the preventive and mitigative measures. The initial literature search yielded 463 articles from different databases. However, 24 were synthesized after others were excluded due to several factors. The analysis revealed several techniques that organizations can adopt to avert ransomware attacks. These approaches include user training and awareness, access control measures, using data backups, and establishing cybersecurity policies in organizations. Most of these approaches are not as effective in mitigating cyberattacks. Hence, this study recommends combining several approaches to ensure maximum protection of computers, systems, devices, and networks in organizations. Individual users can also adopt measures like data encryption, regular updating of computer hardware, blocking pop-up ads, avoiding opening untrusted files or links, and using strong passwords to protect their devices from ransomware attacks.

References

[1] Adam, S. (2021, April 27). *The State of Ransomware 2021*. Sophos News. https://news.sophos.com/en-us/2021/04/27/the-state-of-ransomware-2021/#:~:text=Based%20on%20findings%20from%20an

[2] Alansari, M. M. H., Aljazzaf, Z. M., & Sarfraz, M. (2019). On Cyber Crimes and Cyber Security. *Developments in Information Security and Cybernetic Wars*, 1–41. https://doi.org/10.4018/978-1-5225-8304-2.ch001

[3] Alshaikh, H., Ramadan, N., & Ahmed, H. (2020). Ransomware Prevention and Mitigation Techniques. *International Journal of Computer Applications*, *177*(40), 31–39. https://doi.org/10.5120/ijca2020919899

[4] Ami, O., Elovici, Y., & Hendler, D. (2018). Ransomware prevention using application authentication-based file access control. *Proceedings of the 33rd Annual ACM Symposium on Applied Computing - SAC '18*. https://doi.org/10.1145/3167132.3167304

[5] Bajpai, P., & Enbody, R. (2020). Attacking Key Management in Ransomware. *IT Professional*, *22*(2), 21–27. https://doi.org/10.1109/mitp.2020.2977285

[6] Bajpai, P., Enbody, R., & Cheng, B. H. C. (2020). Ransomware Targeting Automobiles. *Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security*. https://doi.org/10.1145/3375706.3380558

[7] Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*, *111*(1). https://doi.org/10.1016/j.cose.2021.102490

[8] Cabaj, K., & Mazurczyk, W. (2016). Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall. *IEEE Network*, *30*(6), 14–20. https://doi.org/10.1109/mnet.2016.1600110nm

[9] Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *SA Journal of Information Management*, *23*(1). https://doi.org/10.4102/sajim.v23i1.1277

[10] Chung, M. (2019). Why employees matter in the fight against ransomware. *Computer Fraud & Security*, *2019*(8), 8–11. https://doi.org/10.1016/s1361-3723(19)30084-3

[11] Connolly, L. Y., Wall, D. S., Lang, M., & Oddson, B. (2020). An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa023

[12] Erridge, T. (2016). Ransomware: threat and response. *Network Security*, *2016*(10), 17–19. https://doi.org/10.1016/s1353-4858(16)30097-6

[13] Genç, Z. A., Lenzini, G., & Ryan, P. Y. A. (2018). No Random, No Ransom: A Key to Stop Cryptographic Ransomware. *Detection of Intrusions and Malware, and Vulnerability Assessment*, 234–255. https://doi.org/10.1007/978-3-319-93411-2_11

[14] Huang, J., Xu, J., Xing, X., Liu, P., & Qureshi, M. K. (2017). FlashGuard. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. https://doi.org/10.1145/3133956.3134035

[15] Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Ransomware Detection,

Avoidance, and Mitigation Scheme: A Review and Future Directions. *Sustainability*, *14*(1), 8. https://doi.org/10.3390/su14010008

[16] Kharraz, A., & Kirda, E. (2017). Redemption: Real-Time Protection Against Ransomware at End-Hosts. *Research in Attacks, Intrusions, and Defenses*, 98–119. https://doi.org/10.1007/978-3-319-66332-6_5

[17] Kolodenker, E., Koch, W., Stringhini, G., & Egele, M. (2017). PayBreak : Defense Against Cryptographic Ransomware. *ACM Digital Library*. https://doi.org/10.1145/3052973.3053035

[18] Luo, X., & Liao, Q. (2007). Awareness Education as the Key to Ransomware Prevention. *Information Systems Security*, *16*(4), 195–202. https://doi.org/10.1080/10658980701576412

[19] Manjezi, Z., & Botha, R. A. (2019). Preventing and Mitigating Ransomware. *Communications in Computer and Information Science*, *973*, 149–162. https://doi.org/10.1007/978-3-030-11407-7_11

[20] Mansfield-Devine, S. (2017). Ransomware: the most popular form of attack. *Computer Fraud & Security*, *2017*(10), 15–20. https://doi.org/10.1016/s1361-3723(17)30092-1

[21] McIntosh, T., Kayes, A. S. M., Phoebe Chen, Y.-P., Ng, A., & Watters, P. (2021). Dynamic User-Centric Access Control for Detection of Ransomware Attacks. *Computers & Security*, 102461. https://doi.org/10.1016/j.cose.2021.102461

[22] 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. https://doi.org/10.1109/lca.2018.2883431

[23] Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security*, *120*(1), 102820. https://doi.org/10.1016/j.cose.2022.102820

[24] Monika, Zavarsky, P., & Lindskog, D. (2016). Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization. *Procedia Computer Science*, *94*, 465–472. https://doi.org/10.1016/j.procs.2016.08.072

[25] Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA – Journal of Business and Public Administration*, *9*(3), 71–88. https://doi.org/10.2478/hjbpa-2018-0024

[26] Parkinson, S. (2017). Use of access control to minimise ransomware impact. *Network Security*, *2017*(7), 5–8. https://doi.org/10.1016/s1353-4858(17)30069-7

[27] Pope, J. (2016). Ransomware: Minimizing the Risks. *Innovations in Clinical Neuroscience*, *13*(11-12), 37–40. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5300711/#:~:text=Joseph%20Popp%2C%20a%20World%20Health

[28] Saleous, H., Ismail, M., AlDaajeh, S. H., Madathil, N., Alrabaee, S., Choo, K.-K. R., & Al-Qirim, N. (2022). COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. *Digital Communications and Networks*, *9*(1). https://doi.org/10.1016/j.dcan.2022.06.005

[29] Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. *International Cybersecurity Law Review*, *3*(1). https://doi.org/10.1365/s43439-021-00045-4

[30] Sillic, M. (2019). Critical impact of organizational and individual inertia in explaining non-compliant security behavior in the Shadow IT context. *Computers & Security*, *80*, 108–119. https://doi.org/10.1016/j.cose.2018.09.012

[31] Thomas, J. (2018). Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks. *International Journal of Business and Management*, *13*(6), 1–1. https://ideas.repec.org/a/ibn/ijbmjn/v13y2018i6p1.html

[32] Thomas, J. E., & Galligher, G. C. (2018). Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware. *Computer and Information Science*, *11*(1), 14. https://doi.org/10.5539/cis.v11n1p14

[33] Tiu, Y. L., & Zolkipli, M. F. (2021). Study on Prevention and Solution of Ransomware Attack. *Journal of IT in Asia*, *9*(1), 133–139. https://doi.org/10.33736/jita.3402.2021

[34] van Steen, T., Norris, E., Atha, K., & Joinson, A. (2020). What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa019

[35] Wade, M. (2021). Digital hostages: Leveraging ransomware attacks in cyberspace. *Business Horizons*. https://doi.org/10.1016/j.bushor.2021.07.014

[36] Watson, R. T., & Webster, J. (2020). Analysing the past to prepare for the future: Writing a literature review a roadmap for release 2.0. *Journal of Decision Systems*, *26*(2), 1–19. https://doi.org/10.1080/12460125.2020.1798591