INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 14, Issue 1, (2024) E-ISSN: 2222-6990

Evolution and Impact of Ransomware: Patterns, Prevention, and Recommendations for Organizational Resilience

Mahendran Muniandy, Noor Azma Ismail, Abdulaziz Yahya Yahya Al-Nahari & Danny Ngo Lung Yao

School of Information Technology, UNITAR International University, Malaysia

Email: unu2200468@student.unitar.my, azma1706@unitar.my, abdulaziz.yahya@unitar.my, danny.ngo@unitar.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v14-i1/19803 DOI:10.6007/IJARBSS/v14-i1/19803

Published Date: 10 January 2024

Abstract

Ransomware, manifesting as Crypto or Locker, poses a significant threat to fundamental computer systems and infrastructures with the primary goal of extracting financial gain from victims through ransom demands for decryption keys. This paper delves into the evolving landscape of ransomware, a persistent and advancing form of malicious software. Besides, this paper explores the development, patterns, and methods of ransomware attacks, scrutinizing their impact on organizations over time. In addition, this study examines the root causes of ransomware's organizational impact and evaluates its evolving scales. The investigation also addresses proactive measures organizations can adopt, aligning with the cybersecurity standards, to enhance preparedness and awareness. Additionally, the study provides recommendations and preventive measures to mitigate the challenges posed by ransomware attacks.

Keywords: Ransomware, Attack, Cybersecurity.

Introduction

The relentless evolution of malware poses a significant challenge to cybersecurity, with ransomware emerging as a pervasive and destructive threat. Malicious software, designed to disrupt electronic devices, continuously evolves, hindering mitigation efforts. The lack of public disclosure regarding malware attacks, driven by concerns about sensitive information and potential damage to reputation, obstructs collaborative prevention efforts and hampers comprehensive research (Holt & Bossler, 2017; Kapoor et al., 2021). Within this landscape, ransomware stands out as a specific form of malware, strategically employed by hackers to encrypt files and demand ransom. The history of ransomware dates back to the late 1990s, evolving in sophistication and impact over the years (Alqahtani & Sheldon, 2022). This study

explores the multifaceted impact of ransomware on organizations, delving into patterns, prevention strategies, and recommendations for enhancing organizational resilience.

Ransomware, often initiated through phishing attacks exploiting human vulnerabilities, can inflict profound harm on organizations. Beyond financial extortion, it holds organizations criminally accountable for data breaches, compromises technical weaknesses, and can cripple essential resources during an attack. The escalating frequency and sophistication of ransomware attacks underscore the urgent need for organizations to fortify their cybersecurity defences and cultivate resilience in the face of this escalating cyber threat (McAfee, n.d.; Alqahtani & Sheldon, 2022). As ransomware operators refine their disruptive tactics and intensify attacks on critical assets, organizations must proactively adapt, prioritize defence strategies, and mitigate potential disruptions to safeguard their digital infrastructure (Alqahtani & Sheldon, 2022). The escalating prevalence of ransomware, fuelled by low entry barriers and the allure of high rewards, demands a comprehensive understanding of the evolving cyber threat landscape and a strategic shift towards proactive defence mechanisms (Accenture's CIFR team; Alqahtani & Sheldon, 2022). In this context, this study aims to address the overarching problem statements, which are ransomware's emergence as a significant cyber threat across sectors, the role of human error in facilitating ransomware attacks, and the critical need for organizational resilience in the face of escalating cyber threats.

In cybersecurity, the persistent evolution of malware poses an ongoing challenge, constantly testing mitigation efforts. The secrecy enveloping malware attacks, fueled by concerns over sensitive information and potential reputational damage, not only impedes research but also complicates the development of effective countermeasures (Holt & Bossler, 2017; Kapoor et al., 2021). This veil of secrecy extends to ransomware, a potent form of malware encrypting files and demanding a ransom for access. Originating in the late 1990s, ransomware has transformed into a sophisticated tool, initiating a digital arms race between cybercriminals and defenders (Alqahtani & Sheldon, 2022). This paper delves into the historical context, patterns, and preventive strategies against ransomware, intending to enhance understanding and fortify organizational resilience against this continually evolving threat. The objectives of this research are as follows:

- To investigate how ransomware has evolved in terms of its development, attack patterns, and methods employed by attackers.
- To assess the potential impact of ransomware on important infrastructure, including industrial control systems and key sectors like healthcare and transportation.
- To explore proactive cybersecurity measures that organizations can adopt to enhance preparedness and awareness regarding ransomware threats.

Evolvement of Ransomware

Ransomware, a significant threat to users' file access, demands payment for restored control, recognized as a global crisis impacting diverse businesses (Muslim et al., 2019). The first ransomware, AIDS Trojan, or PC Cyborg, emerged in 1989, initiating the malicious software trend, but its attempt to extort users was hindered by limited computer usage. Subsequent developments, including asymmetric ransomware, faced payment challenges, leading to the creation of a deceptive antivirus to protect developers' identities (Muslim et al., 2019).

Ransomware attacks, driven by financial motives, globally employ vectors such as email, spam, and phishing (Pascariu & Barbu, 2019), complicating tracking due to their use of virtual

currencies like Bitcoin for ransom payments. Various notable ransomware variants, including BadRabbit, BitPaymer, Cerber, Cryptolocker, Dharma, DoppelPaymer, GandCrab, Locky, Maze, MeduzaLocker, NetWalker, NotPetya, Petya, REvil, Ryuk, SamSam, and WannaCry, contribute to this evolving threat landscape (CrowdStrike, 2022).

Ransomware, differing from conventional malware, stands out with explicit actions of system locking, file encryption, and ransom note display, conveying infection details and the required ransom for recovery (Swami et al., 2021). Its attack cycle encompasses stages like exploitation, infection, delivery, execution, backup tampering, file encryption, user notification, and cleanup (Pascariu & Barbu, 2019).

The surge in ransomware is linked to its adoption by cybercriminals pursuing notoriety and financial gains, aligning it with crimeware—a category of malicious software for criminal internet activities and cyber extortion (Zakaria et al., 2017). The intricate recovery process from ransomware, compounded by its categorization as scareware, underscores the multifaceted challenges posed by this cyber threat (O'Kane et al., 2018). Despite the frequent release of numerous ransomware variants, each derived from its forerunner, the classification of ransomware families remains pivotal for effective response strategies (Kiru & Jantan, 2020).

Transitioning to the modern era, Trojan.Gpcoder, a ransomware variant featuring a flawed symmetric encryption mechanism had risen. Disseminated through deceptive spam emails masquerading as job applications, it represented one of the initial instances of ransomware crafted by Russian criminal organizations, impacting individuals in Russia and neighboring nations (Cawley, 2016). Later, an upswing in ransomware popularity, brought forth Trojan.Cryzip and Trojan.Archiveus. While the former generated password-protected archives of data files, the latter demanded a drug purchase from designated online pharmacies for password retrieval, reflecting early efforts to monetize ransomware (Kiru & Jantan, 2020; O'Kane et al., 2018).

Afterward, Locker Ransomware went global, presenting explicit images and demanding payment through SMS or premium phone calls, extending ransomware attacks from Russia to the United States and Europe (Richardson, Ronny, & MaxM, 2017). Later, the Trojan variant GPcode employed a 1024-bit RSA key and requested payment in e-gold or Liberty Reserve, showcasing early sophistication in ransomware operations and payment methods (Richardson et al., 2017).

In 2011, a significant surge in ransomware incidents occurred, driven by the establishment of anonymous payment methods, with a quarterly rise in new samples showcasing the escalating threat and adaptability of ransomware developers (Richardson et al., 2017). Variants like Reveton and Trojan.Randsom.C introduced diverse coercive tactics, signifying a shift and diversification in ransomware strategies (Hassan, 2019; Savage et al., 2015).

In 2013, a resurgence in crypto ransomware emerged, overshadowing locker ransomware and showcasing increased potency in notable variants demanding $300 in payment, signaling a shift in ransomware preferences (Richardson et al., 2017). The infamous CryptoLocker, credited to hacker Slavik in August 2013, marked a milestone, utilizing victims' cryptographic keys for encryption and propagating through the Gameover ZeuS botnet via deceptive emails. Its three-day payment window, demanding one Bitcoin, and alternative payment options like MoneyPak and Paysafecard reflected a strategic shift in ransomware tactics. Operation Tovar, a collaborative effort, successfully shut down CryptoLocker's servers, providing victims with free decryption services. CryptoDefense, earning $34,000 in its debut month, and the evolved CryptoWall, exploiting a Java vulnerability and leading to a nearly one-million-dollar ransom

payment, further underscored the evolving landscape of ransomware threats (Hassan, 2019; Richardson et al., 2017).

The rise of ransomware-as-a-service allowed attackers to build ransomware through TOR-accessible websites, exemplified by LockerPin targeting Android devices, highlighting the expanding reach of ransomware. The Cyber Threat Alliance estimated total ransomware damage at $325 million, and identified Linus.Encoder.1 targets Linux-based systems (Hassan, 2019; Richardson et al., 2017). Locky ransomware's update, coupled with FBI estimates of $209 million in ransomware revenue for Q1 2016, emphasized the financial success of such attacks, with notable variants including TorrentLocker, CryptoWall, and CTB-Locker (Richardson et al., 2017). The trend of enhancing existing strains rather than creating new ones was showcased by the emergence of Goldeneye and Petya (NotPetya) (Richardson et al., 2017). In 2020, Ragnar Locker attacked CWT, leading to a ransom payment after compromising confidential files and impacting 30,000 enterprise computers (Ahmed, 2019).

The seventh-largest U.S. commercial insurer, CNA Financial, experienced a sophisticated cybersecurity attack orchestrated by the Phoenix group, using the Phoenix Locker ransomware (Ali, 2017; Ahmed, 2019).

Law enforcement and cybersecurity firms, such as Symantec, are increasing efforts against ransomware, leading criminals to adapt. The use of Tor, the Invisible Internet Project (I2P), and cryptocurrencies like Bitcoin is growing, complicating tracking efforts. Ransomware, expanding to Apple and Android systems, poses threats to the Internet of Things (IoT), evident in attacks on smart thermostats and mobile devices. Researchers showcasing control over moving vehicles highlight the potentially life-threatening consequences of ransomware, emphasizing the need for vigilance (Ahmed, 2019; Ali, 2017; Richardson et al., 2017).

Targeting businesses for lucrative gains, cybercriminals leverage the low-risk, high-reward model of crypto-ransomware. Osterman Research, Inc. reveals that 79% of U.S. corporate organizations faced ransomware incidents where the prime targets include the healthcare, financial services, manufacturing, and government sectors (Ali, 2017; State of Ransomware, 2016). The aftermath extends beyond financial demands, with reported disruptions, employee reliance on personal devices during downtime, and revenue losses. The emerging tactic of threatening to make stolen files public adds complexity and potential embarrassment for victims (Richardson et al., 2017).

Continually refining their techniques, ransomware perpetrators incorporate delayed notifications, threaten public exposure, and utilize alternative attack methods. The SVG files and Word macros had been used as additional offensive tools (Gallagher, 2016c; Rosenquist, 2016). Recent developments indicate a regionalized focus, with businesses capable of substantial ransom payments being prime targets. Criminals employ detection-evasion tactics, including CAPTCHA tests, showcasing the increasing sophistication of their operations (Constantin, 2015; Mohammad, 2020). North Korea's attack on Sony Pictures demonstrated the potential use of ransomware as a weapon, emphasizing the need for robust cybersecurity measures to counter its weaponization (Ali, 2017).

Understanding the history of ransomware reveals conflicting accounts regarding its origins and spread, with some attributing it to Russia and Eastern Europe and others presenting different timelines and origins, creating a nuanced narrative that underscores the evolution from unsophisticated attacks to sophisticated, targeted operations and the need for a comprehensive understanding of its historical context (Maurya et al., 2018).

The inception of ransomware witnessed a shift in cybercriminal tactics, including luring users to malicious websites and encrypting files for extortion. Concurrently, ransomware strategies

evolved towards regionalized attacks on financially robust businesses, with criminal groups strategically targeting sectors, employing malware encryption and data exfiltration, compelling companies to balance hefty ransom payments against the risk of exposing sensitive information (Maurya et al., 2018; Ozer et al., 2019). Understanding this evolution, monitoring ransomware patterns, and assessing their impact on the Bitcoin ecosystem are crucial for analyzing and mitigating cyber threats, emphasizing the interplay between ransomware attacks and cryptocurrency transactions (Turner et al., 2020).

Ransomware imposed a staggering $20 billion global economic cost, projected to reach $265 billion by 2031, reflecting its exponential growth and financial impact (Kochovski, 2021). This underscores the urgent need for robust cybersecurity measures and proactive strategies to combat the increasing sophistication and financial repercussions of ransomware attacks.

Impact on the Organization

Despite increasing awareness of ransomware threats, businesses, irrespective of size or industry, remain inadequately prepared, making them lucrative targets for cybercriminals; with a focus shift to smaller enterprises, these attacks have become more widespread and destructive annually (Zakaria et al., 2017). Malwarebytes' study reveals alarming facts, indicating that nearly one-fifth of businesses experienced ransomware attacks and over a third reported financial losses, emphasizing the urgent need for enhanced cybersecurity measures and proactive strategies to counteract the escalating threat landscape (Maurya et al., 2018; Yuryna Connolly et al., 2020).

Ransomware employs diverse methods of attack, including exploit kits, malicious email attachments, and links, with victims often receiving spam emails notifying them of computer lockdowns (Maurya et al., 2018; Kiru & Jantan, 2020). Opening email attachments or clicking on malicious links can lead to automatic ransomware downloads, compromising systems and files, followed by ransom demands (Richardson & North, 2017; Kiru & Jantan, 2020). Phishing, especially spear phishing, remains a prevalent technique, enabling criminals to gather sensitive information for potential public exposure, while drive-by downloads exploit software vulnerabilities to secretly infect systems (Connolly et al., 2020; Hassan, 2019). The consequences of ransomware attacks are profound, encompassing short-term disruptions in operations, productivity losses, mitigation expenses, and ransom payments, as well as potential long-term impacts like revenue decline, brand reputation damage, employee layoffs, client and partner loss, and, in extreme cases, business shutdowns (Hassan, 2019).

Ransomware incidents have inflicted significant financial losses on major organizations, such as FedEx's reported $300 million due to NotPetya in 2017 and Atlanta spending over $2.6 million on a SamSam ransomware attack in 2018, while Cognizant Technology Solutions reported reduced profitability in 2020 following a Maze ransomware assault, and the City of Baltimore spent over $18 million rebuilding its IT network after a SamSam attack (Hassan, 2019). Despite the proliferation of scholarly research on ransomware focusing on technical aspects, including detection and prevention systems, a paucity of research examines the socio-technical dimensions or the experiences of victimized organizations, emphasizing the need for comprehensive preventative measures (Yuryna Connolly et al., 2020; Holt & Bossler, 2017; Hassan, 2019). While the frequency of ransomware attacks against enterprises is increasing, it remains challenging to measure accurately, with varying statistics globally, indicating the complex nature of cybercrime victimization and the evolving threat landscape (Alshaikh et al., 2020; Shalaginov et al., 2020; Ahmed, 2019). Small and medium-sized enterprises (SMEs) often underestimate their vulnerability, with the entrepreneurial nature

of SMEs contributing to risk-taking behavior, underscoring the importance of acknowledging equivalent risk levels and implementing robust cybersecurity measures (Bamrara, 2018; Smith, 2017; Kurpjuhn, 2015).

Ransomware attacks have shifted from opportunistic targeting of individuals to more lucrative and targeted assaults on larger organizations, with perpetrators focusing on sectors like government, military, education, research, healthcare, retail, and wholesale (Bamrara, 2018). Despite no clear correlation between organization size and cybercrime victimization rates, larger organizations may face higher infection risks due to human errors (Bergmann MC, 2017; Richardson & North, 2017). The decision to pay a ransom remains a complex dilemma, with the threat's psychological impact often as potent as the actual malware damage (Muslim et al., 2019; Kumar et al., 2016).

Businesses, especially those in the financial sector, emergency services such as law enforcement, fire departments, hospitals, and private sector organizations are prominent targets for ransomware attacks due to the valuable data they hold, the potential for significant consequences, and the vulnerabilities in their security systems, leading to potential financial losses, reputational damage, and customer loss (Maurya et al., 2018; Shalaginov et al., 2020; Kumar et al., 2016; Connolly et al., 2020).

In 2021, more organizations experienced ransomware attacks compared to 2020, possibly driven by the ransomware-as-a-service model's popularity, which lowers technical barriers. The encryption success rate rose, and the extortion-only attack incidence dropped, indicative of an evolving and more challenging threat landscape (Sophos, 2021; Kumar et al., 2016; Shalaginov et al., 2020). The impact of ransomware extends beyond financial costs, for instance, significant disruptions to operations, loss of business/revenue, and expenditure for mitigation (Kumar et al., 2016; Shinde et al., 2016; Sen & Chourey, 2020). Recovery times varied, with higher education and central/federal government sectors taking over a month, while manufacturing and financial services recovered the fastest, emphasizing the importance of comprehensive recovery planning (Sen & Chourey, 2020). Notably, most organizations relying on backups and cyber insurance for protection lack preventative measures, highlighting the need for updated defense strategies (Kumar et al., 2016).

The escalating threat of ransomware is evident in the doubling of affected organizations with improvements in response capabilities; however, the average proportion of encrypted data restored post-payment has fallen and the incidence of victims paying ransomware has nearly tripled. Addressing this challenge requires strategic investments in technology, skills, and knowledge, as simply allocating resources is insufficient (Shinde et al., 2016; Sen & Chourey, 2020; Kumar et al., 2016). Notably, cyber insurance plays a crucial role in mitigating financial risks, but the increasing difficulty in obtaining coverage prompts organizations to enhance their cyber defences to bolster their insurance position (Sen & Chourey, 2020). The global impact of ransomware is exemplified by significant incidents such as the 2019 RobinHood attack on Baltimore, the 2021 Colonial Pipeline ransomware outbreak, and the 2021 Health Service Executive attack in Ireland, underscoring the pervasive and damaging nature of these attacks across diverse sectors (Yilmaz et al., 2022; Shalaginov et al., 2020). In 2022, the Ministry of Finance of Costa Rica experienced a ransomware attack, causing economic disruptions, even though the government refused to negotiate, highlighting the ongoing challenges posed by these threats (Shalaginov et al., 2020).

The US financial institutions paid more ransomware-related payments than in previous years, signalling the escalating impact of ransomware, particularly from Russian criminal groups (Gillum, 2022). Regarding the impact of ransomware on organizations (Shinde et al., 2016),

potential ramifications include business shutdowns for days or weeks, loss of sales and client confidence, the challenging decision of whether to pay the ransom, reputational damage, and regulatory fines, as illustrated by the recent ransomware attack on Continental, a German international automobile business, by the LockBit group. This case involves the theft of information, threats of online exposure, and potential negotiations or resistance to complying with the ransom demands, reflecting the complex and damaging nature of contemporary ransomware attacks (Shalaginov et al., 2020; Smith, 2022).

Implementation and Analysis

The survey was published online at *allcounted.com* with the intention of receiving at least 50 responses from working adults, but 77 attempts were received. Only 58 of the 77 respondents completed the survey, and the discussion data will be drawn solely from the 58 completed surveys which is filtered to working adults which is targeted at 'Public Sector, Private Sector & Own Business' only. The filter returned 53 respondents. The data will be used further in this discussion will be based on 53 respondents only.

Demographic Data

The survey was completed by employed adults from various sectors. It is observed that 83.02% of the contributions come from working individuals in the "Private Sector." And remaining is from 'Own Business' and the lowest one is from 'Public Sectors'. From this it can be decided that 'Private Sector' will be contributing major influence over the topic discussions. Demographic data is presented in Table 1.

Table 1
Summary of Survey Result from Section A (Demographic Data)

Survey Questions	Options	Respondent	Percentages %
Are you Working Adults	Yes	53	100.00%
	No		
Your Gender	Male	30	56.60%
	Female	23	43.40%
Your Age Range	18 - 25	7	13.21%
	26 - 30	8	15.09%
	31 - 50	38	71.70%
Your Working Organization Types	Public Sector	4	7.55%
	Private Sector	44	83.02%
	Own Business	5	9.43%
	Others		
	Not Applicable		
Your Occupation Level	Clerical	1	1.89%
	Executive	20	37.74%
	Managerial	24	45.28%
	Others	8	15.09%
	Not Applicable		
Your Working Experience	Less then 2 Years	3	5.66%
	2 to 5 Years	10	18.87%
	6 to 10 Years	11	20.75%
	More than 10 Years	29	54.72%
	Not Applicable		

Evolvement of Ransomware

There are a total of six questions presented to assess the awareness level of working adults; the results are positive, and most respondents provided positive responses. Which shows they are aware of what is 'Ransomware'. Except for one question pertaining to inception of 'Ransomware' from Question 10, it was observed that a high percentage (75.47%) of respondent did not know that ransomware existed since 1989. The breakdown of a total of 6 questions and its responses summary are summarized in Table 2.

The awareness level of working individuals is measured using a total of six questions; most respondents gave favourable answers, and the results are encouraging which demonstrates their knowledge of what "ransomware" is. With the exception of one question about the origins of "Ransomware" in Question 10, it was found that a substantial portion of respondents (75.47%) were unaware that ransomware had been around since 1989. Table 2 provides an overview of the six questions that were asked and a summary of the answers.

Table 1
Summary of Survey Result from Section B (Evolvement of Ransomware)

Survey Questions	Options	Respondent	Percentages %
7) Do you know what Ransomware is ?	Yes	46	86.79%
	No	7	13.21%
8) Do you aware on Ransomware impact if being attacked?	Yes	46	86.79%
	No	7	13.21%
9) In your opinion, which of following is being mostly targeted for ransomware attack ?	Individual	3	5.66%
	Organisation	21	39.62%
	Both	29	54.72%
10) Do you know that Ransomware is exist since 1989 ?	Yes	13	24.53%
	No	40	75.47%
11) Do you know that Ransomware is not limited to one type but many variances?	Yes	43	81.13%
	No	10	18.87%
12) Do you feel that the ransomware attack negatively impacts your organisation reputation?	Yes	47	88.68%
	No	6	11.32%

Preventive Measures

A total of six survey questions about "Ransomware" were developed by "Deloitte" and given to fifty-three working adults. Remarkably, positive answers to most of the queries show that the company is in fact well-prepared for "Ransomware" attacks. "Deloitte" cyber security experts strongly advise the mitigating techniques that are identified in the survey. Presumably, most of the companies who participated in the study, especially those from "Private Sectors," showed that they had adequate safeguards in place to guard against cyberattacks. The results are summarised in Table 3.

Table 2
Summary of Survey Result from Section C (Preventive Measures)

Survey Questions	1 - No, and not considered		2 - No, but considered		3 - No		4 - Yes	
	Respondent	Percentages %	Respondent	Percentages %	Respondent	Percentages %	Respondent	Percentages %
13) Has your organization identified the most critical business processes that depend on technology? *What are they? Who owns them? This analysis needs to be narrowed down to those core processes that simply can't operate effectively without the technology.*	1	1.89	11	20.75%	6	11.32%	35	66.04%
14) For these critical business processes, is there a comprehensive 'tree of dependencies' that covers technology systems, suppliers, and people? *It is vital to understand this mapping as it allows an organization to pinpoint the components that have the potential to cause system failures or to introduce ransomware. And start executing the resulting failure scenarios.*	3	5.66%	12	22.64%	5	9.43%	33	62.26%
15) Is cyber risk owned by your organization's business leaders, and do they operate together, collaboratively, and effectively? *This is frequently an issue in organizations where ineffective cyber risk management leads to serious vulnerabilities remaining unresolved. This happens when formal decisions around accepting risk or funding remediation are isolated, uncoordinated, or simply not made – and so not acted on.*	1	1.89%	8	15.09%	10	18.87%	34	64.15%
16) Is your organization proactively managing the risk of key suppliers involved in critical processes and systems? *Suppliers can inadvertently introduce ransomware and other malware in core OT systems. Many operate with outdated contracts that lack accountability or clarity around responsibilities for cyber security controls. Identifying such suppliers, assessing their cyber security controls, and monitoring their effectiveness are all key ways to avoid opening up further attack vectors and risks to critical systems.*	1	1.89%	11	20.75%	5	9.43%	36	67.92%
17) Does legacy critical systems being protected ? *Unsupported software and devices from legacy industrial control systems are vulnerable to common malware, let alone targeted attacks. Many legacy employees with the system's 'know how' may have already left the organization. In some cases, the incident recovery team has to rebuild using year-old backup data. Organizations need to decide how to protect legacy systems and be prepared to rebuild industrial processes from scratch—including these systems.*	2	3.77%	9	16.98%	8	15.09%	34	64.15%
18) Has sufficient crisis management and recovery testing been done for a ransomware attack on a critical system? *It is still common for organizations that attempt a system restoration from backups to discover it is much harder than expected (or that the backups are inoperative or also infected with ransomware). Organizations need to thoroughly practice response processes – including rebuilding systems from scratch – with their management teams, suppliers, and other third parties. In this way, they can remediate technical issues, identify what information is needed and who is responsible to respond effectively, align leadership and develop muscle memory around decision-making, and clarify how to communicate with regulators, customers, and the media.*	2	3.77%	11	20.75%	10	18.87%	30	56.60%

Impact to the Organisations

Eight questions from "ransomware.org" were posted in order to get opinions on "Ransomware impact to the organisation," and Table 4 shows the varied opinions of working adults that were obtained.

Table 4
Summary of Survey Result from Section D (Impact to the Organisation)

Survey Questions	Options	Respondent	Percentages %
19) In your opinion, what would be most effective step in ending the scourge of ransomware?	There's nothing that can be done. Ransomware is here to stay	8	15.09%
	Less Government involvement	-	-
	More Government involvement	16	30.19%
	More public/private partnerships to end ransomware	28	52.53%
	Regulating Cryptocurrency	10	18.87%
	Better defenses	37	69.81%
	None of the above	2	3.77%
20) In the event of an attack, I know exactly what to do and who to contact.	Yes	32	60.38%
	No	21	39.62%
21) Does your organization have a disaster recovery plan?	Yes, but it's not documented. We just know what we'll do	8	15.09%
	Yes, it's documented, and we update it regularly	32	60.38%
	Yes, but it needs updating	11	20.75%
	No	2	3.77%
22) Does your organization have an incident response plan?	Yes, but it needs updating	18	33.96%
	Yes, but it's not documented. We just know what we'll do	5	9.43%
	Yes, it's documented, and we update it regularly	24	45.28%
	No	6	11.32%
23) If your organization experienced a ransomware attack, what area of your business do you suspect would be most negatively impacted?	IT infrastructure	35	66.04%
	Human resources	7	13.21%
	Customer trust	21	39.62%
	Marketing	9	16.98%
	Cash Flow	15	28.30%
	Accounting	19	35.85%
	Operations	25	47.17%
	Sales	19	35.85%
	Our reputation	26	49.06%
	No idea	7	13.21%
24) Has your organization ever experienced a ransomware event?	Yes	11	20.75%
	No	28	52.83%
	I'm not sure	14	26.42%
25) In your opinion – is ransomware a real business threat, or is it over-hyped?	It's over-hyped	4	7.55%
	A business threat but not to my organization	13	24.53%
	Significant business threat	36	67.92%
26) If your organization experienced a ransomware attack, how long do you estimate it would take to get back to business as normal?	Hours – we're "boy-scout" level prepared	12	22.64%
	Days – we're prepared but conservative in our estimate	26	49.06%
	Weeks – we're not prepared enough	5	9.43%
	Months – we have little to no preparation	5	9.43%
	Likely prove devastating to our business	5	9.43%

Most of the responses relevant to the recommended answer have received a higher percentage, indicating that the impact is well understood by the organisations and that mitigation is in place for most organisations. Those working adults understand what 'Ransomware' is and the impact associated.

Conclusion and Recommendations

Conclusion

It is hardly surprising that ransomware will evolve over the next few years. If ransomware is not taken seriously, it will be more than simply a software capable of disrupting entire organisation infrastructure; it will have the power to disable an entire city or perhaps a country until the desired ransom is paid (Muslim et al., 2019). Cyber criminals are likely to employ tactics such as hacking industrial control systems (ICS) and other key infrastructure in order to disable ecosystems rather than just networks. Payment systems such as E-bay are among the few possible targets for cyber attackers. In 2016, there was a transit attack in which ransomware targeted a service provider's kiosk. Ransomware has already targeted hospitals and transportation providers. In the future, attackers will be able to target larger targets such as industrial robots that are frequently utilised in manufacturing or infrastructure sectors that connect smart cities (Muslim et al., 2019).

Ransomware can be costly and devastating to a company that does not actively protect itself or is unprepared for the consequences of an attack. As this form of attack becomes more common and evolves, it is vital that organisations are aware of the most recent effective attack patterns and what they can do to avoid vulnerability. Organizations can reduce the likelihood of a successful Ransomware attack and limit related risks in terms of response effort, downtime, costs, organisational impact, and reputation damage by implementing best practices recommendations.

Recommendations

Ransomware has evolved over time because of the lucrative method of forcing victims to pay a ransom. It is worth noting that we can implement preventive procedures in our organisations to deal with such situations if they emerge. The following are highly suggested preventive measures that an organisation should prioritise (Deloitte, An anti-ransomware strategy - deloitte 2020)

1. Implementing and configuring an email gateway to scan and block malicious email, including embedded links and attachments.
2. Implementation of URL filtering and blocking within organisation networks which giving access to public network.
3. Implements Sender Policy Framework ("SPF"), Reporting & Conformance ("DMARC") and Domain based Message Authentication which can reduce incoming spoof emails.
4. Configure organisation firewall to block malicious IP addresses.
5. Provide cyber security awareness training once a year which emphasizes on cyber incidents.
6. Employees should be randomly tested to see if they are vulnerable to phishing campaigns, and if so, further resources and training should be provided to those who struggle.
7. Tag external emails with a notice that they come from outside the organisation to raise employee awareness.
8. Implement Business Continuity & Incident Response Plans
9. Incorporate Endpoint Detection & Response (EDR) with Antivirus
10. Have a regular backup of important data frequently.
11. Review the access controls.
12. Patch the unpatched system regularly.

Future Works

The author of this study article examined the effects of ransomware on organisations as well as how it has changed over time since its invention. Research has shown that no antivirus programme or other kind of security can completely prevent ransomware attacks. It indicates that the effect is there and getting stronger over time.

In the future, the author plans to create a machine learning approach based on artificial intelligence (AI) to safeguard organisations. This approach will be able to recognise ransomware and take the appropriate precautions to prevent becoming a victim.

Acknowledgement

The authors thank UNITAR International University for the publication of this research.

References

Abulela, M. A., & Harwell, M. (2020). Data Analysis: Strengthening Inferences in Quantitative Education Studies conducted by novice researchers. *Educational Sciences: Theory & Practice*, *20*(1), 59–78. https://doi.org/10.12738/jestp.2020.1.005

Adamov, A., & Carlsson, A. (2017). The state of ransomware. trends and mitigation techniques. *2017 IEEE East-West Design & Test Symposium (EWDTS)*. https://doi.org/10.1109/ewdts.2017.8110056

Ahmed, M. R. (2019). Ransomware: The evolution of a cybercrime. *International Journal of Psychosocial Rehabilitation*, *23*(4), 1228–1237. https://doi.org/10.37200/ijpr/v23i4/pr190449

Ali, A. (2017). Ransomware: A research and a personal case study of dealing with this nasty malware. *InSITE Conference*. https://doi.org/10.28945/3661

Alqahtani, A., & Sheldon, F. T. (2022). A survey of Crypto Ransomware Attack Detection Methodologies: An evolving outlook. *Sensors*, *22*(5), 1837. https://doi.org/10.3390/s22051837

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

Aslan, P. O. (2022). Ransomware detection in cyber security domain. *Bitlis Eren Üniversitesi Fen Bilimleri Dergisi*, *11*(2), 509–519. https://doi.org/10.17798/bitlisfen.1038966

Bamrara, A. (2018). Identifying and analyzing the latent cyber threats in developing economies. *Cyber Security and Threats*, 1044–1059. https://doi.org/10.4018/978-1-5225-5634-3.ch051

Chowdhury, N. (2019). Bitcoin: World's first cryptocurrency. *Inside Blockchain, Bitcoin, and Cryptocurrencies*, 61–89. https://doi.org/10.1201/9780429325533-4

Faghihi, F., & Zulkernine, M. (2021). RansomCare: Data-centric detection and mitigation against smartphone crypto-ransomware. *Computer Networks*, *191*, 108011. https://doi.org/10.1016/j.comnet.2021.108011

Hassan, N. A. (2019). Enterprise defense strategies against ransomware attacks. *Ransomware Revealed*, 115–154. https://doi.org/10.1007/978-1-4842-4255-1_5

Hassan, N. A. (2019). Ransomware distribution methods. *Ransomware Revealed*, 29–46. https://doi.org/10.1007/978-1-4842-4255-1_2

Hassan, N. A. (2019). Ransomware families. *Ransomware Revealed*, 47–68. https://doi.org/10.1007/978-1-4842-4255-1_3

Hassan, N. A. (2019). Responding to ransomware attacks. *Ransomware Revealed*, 203–212. https://doi.org/10.1007/978-1-4842-4255-1_9

Holt, T. J., & Bossler, A. M. (2017). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge, Taylor & Francis Group.

Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: Views from a predictive model and human responses. *Crime Science*, *8*(1). https://doi.org/10.1186/s40163-019-0097-9

Jenkinson, A. (2022). CNA ransomware attack and Cyber Insurance. *Ransomware and Cybercrime*, 29–37. https://doi.org/10.1201/9781003278214-5

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

Kaur, G., Dhir, R., & Singh, M. (2017). Anatomy of ransomware malware: Detection, analysis and reporting. *International Journal of Security and Networks*, *12*(3), 188. https://doi.org/10.1504/ijsn.2017.084399

Kiru, M. U., & Jantan, A. (2020). Ransomware evolution: Solving ransomware attack challenges. *The Evolution of Business in the Cyber Age*, 193–229. https://doi.org/10.1201/9780429276484-9

Kothari, C. R., & Garg, G. (2019). *Research methodology: Methods and techniques*. New Age International (P) Limited, Publishers.

Koutsokostas, V., & Patsakis, C. (2021). Python and malware: Developing stealth and evasive malware without obfuscation. *Proceedings of the 18th International Conference on Security and Cryptography*. https://doi.org/10.5220/0010541501250136

Kumar, S., Madhavan, L., Nagappan, M., & Sikdar, B. (2016). Malware in pirated software: Case study of malware encounters in personal computers. *2016 11th International Conference on Availability, Reliability and Security (ARES)*. https://doi.org/10.1109/ares.2016.101

Kurpjuhn, T. (2015). The SME Security Challenge. *Computer Fraud & Security*, *2015*(3), 5–7. https://doi.org/10.1016/s1361-3723(15)30017-8

Lind, D. A., Marchal, W. G., & Wathen, S. A. (2021). *Statistical techniques in business and Economics*. McGraw-Hill Education.

Maurya, A. K., Kumar, N., Agrawal, A., & Khan, R. A. (2018). Ransomware evolution, target and safety measures. *International Journal of Computer Sciences and Engineering*, *6*(1), 80–85. https://doi.org/10.26438/ijcse/v6i1.8085

Mohammad, A. H. (2020). Ransomware evolution, growth and recommendation for detection. *Modern Applied Science*, *14*(3), 68. https://doi.org/10.5539/mas.v14n3p68

Muslim, A. K., Mohd Dzulkifli, D. Z., Nadhim, M. H., & Haizal Abdellah, R. (2019). A Study of Ransomware Attacks: Evolution and Prevention. *JOURNAL OF SOCIAL TRANSFORMATION AND REGIONAL DEVELOPMENT*, *1*(1), 18–25.

Nyikes, Z., & Szűcs, E. (2019). Prevention of ransomware attacks by increasing security awareness. *Műszaki Tudományos Közlemények*, *11*(1), 149–152. https://doi.org/10.33894/mtk-2019.11.33

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. *IET Networks*, *7*(5), 321–327. https://doi.org/10.1049/iet-net.2017.0207

Ozer, M., Varlioglu, S., Gonen, B., & Bastug, M. (2019). A prevention and a traction system for ransomware attacks. *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*. https://doi.org/10.1109/csci49370.2019.00032

Pascariu, C., & Barbu, I.-D. (2019). Ransomware honeypot: Honeypot solution designed to detect a ransomware infection identify the ransomware family. *2019 11th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*. https://doi.org/10.1109/ecai46879.2019.9042158

Richardson, R., & North, M. (2017). Ransomware: Evolution, Mitigation and Prevention. *Management & Entrepreneurship Department Information Systems Department*, *13*(1), 10–21.

Rubin, H. J., & Rubin, I. S. (2005). *Qualitative interviewing: The Art of Hearing Data*. SAGE.

Security awareness on ransomware threats detection and their protection techniques. (2021). *International Journal of Advanced Trends in Computer Science and Engineering*, *10*(2), 975–983. https://doi.org/10.30534/ijatcse/2021/701022021

Sen, S. K., & Chourey, N. (2020). *A Study of Ransomware Detection and Prevention at Organizations*, *07*(07), 4686–4691.

Shalaginov, A., Dyrkolbotn, G. O., & Alazab, M. (2020). Review of the malware categorization in the era of changing cybethreats landscape: Common approaches, challenges and future needs. *Malware Analysis Using Artificial Intelligence and Deep Learning*, 71–96. https://doi.org/10.1007/978-3-030-62582-5_3

Shinde, R., Van der Veeken, P., Van Schooten, S., & van den Berg, J. (2016). Ransomware: Studying transfer and mitigation. *2016 International Conference on Computing, Analytics and Security Trends (CAST)*. https://doi.org/10.1109/cast.2016.7914946

Shukla, M., Mondal, S., & Lodha, S. (2016). Poster. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. https://doi.org/10.1145/2976749.2989051

Slevitch, L. (2011). Qualitative and quantitative methodologies compared: Ontological and epistemological perspectives. *Journal of Quality Assurance in Hospitality & Tourism*, *12*(1), 73–81. https://doi.org/10.1080/1528008x.2011.541810

Swami, S. L., Punia, P. M., & Swami, M. N. (2021). Ransomware detection system and analysis using latest tool. *International Journal of Advanced Research in Science, Communication and Technology*, 600–608. https://doi.org/10.48175/ijarsct-1683

Teichmann, F. M., & Wittmann, C. (2022). When is a law firm liable for a data breach? an exploration into the legal liability of ransomware and Cybersecurity. *Journal of Financial Crime*. https://doi.org/10.1108/jfc-04-2022-0093

Teymourlouei, H., & Harris, V. E. (2021). Detecting ransomware automated based on network behavior by using Machine Learning. *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*. https://doi.org/10.1109/csci54926.2021.00186

Thakur, S., Chaudhari, S., & Joshi, B. (2022). Ransomware: Threats, identification and prevention. *Cyber Security and Digital Forensics*, 361–387. https://doi.org/10.1002/9781119795667.ch16

Tonidandel, S., Braddy, P. W., & Fleenor, J. W. (2012). Relative importance of managerial skills for predicting effectiveness. *Journal of Managerial Psychology*, *27*(6), 636–655. https://doi.org/10.1108/02683941211252464

Turner, A. B., McCombie, S., & Uhlmann, A. J. (2020). Discerning payment patterns in bitcoin from ransomware attacks. *Journal of Money Laundering Control*, *23*(3), 545–589. https://doi.org/10.1108/jmlc-02-2020-0012

Taherdoost, H. (2016). Validity and reliability of the research instrument; how to test the validation of a questionnaire/survey in a Research. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3205040

Yadav, S. (2022). A survey on ransomware malware and ransomware detection techniques. *International Journal for Research in Applied Science and Engineering Technology*, *10*(1), 243–248. https://doi.org/10.22214/ijraset.2022.39787

Yilmaz, Y., Cetin, O., Grigore, C., Arief, B., & Hernandez-Castro, J. (2022). Personality types and ransomware victimisation. *Digital Threats: Research and Practice*. https://doi.org/10.1145/3568994

Connolly, Y. A., & Borrion, H. (2022). Reducing ransomware crime: Analysis of Victims' payment decisions. *Computers & Security*, *119*, 102760. https://doi.org/10.1016/j.cose.2022.102760

Connolly, Y. L., 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

Zakaria, W. Z., Abdollah, M. F., Mohd, O., & Ariffin, A. F. (2017). The rise of Ransomware. *Proceedings of the 2017 International Conference on Software and e-Business - ICSEB 2017*. https://doi.org/10.1145/3178212.3178224