INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

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

Fortifying Against Ransomware: Navigating Cybersecurity Risk Management with a Focus on Ransomware Insurance Strategies

Mujeeb Ur Rehman Shaikh[1], Rafi Ullah[2], Rehan Akbar[3], K. S. Savita[4] and Satria Mandala[5]

[1,2,4]Computer and Information Sciences Department, Universiti Teknologi PETRONAS, Seri Iskandar, 32610, Perak, Malaysia, [1,2,3,4]Positive Computing Research Centre, Universiti Teknologi PETRONAS, Seri Iskandar, 32610, Perak, Malaysia, [3]School of Computing and Information Sciences, Florida International University, Miami, United States of America, [5]Human Centric (HUMIC) Engineering & School of Computing Telkom University Bandung, Indonesia

Corresponding Author Email: mujeeb_22007910@utp.edu.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v14-i1/20566 DOI:10.6007/IJARBSS/v14-i1/20566

Published Date: 15 January 2024

Abstract

This study explores the issue of preventing ransomware attacks using risk management and insurance techniques. Threats from ransomware, which compromise operations, data integrity, and financial stability, have emerged as a major concern for enterprises. The present status of ransomware attacks and their possible effects on organizations are first examined after which we analyse several strategies for reducing the dangers to cyber security posed by these threats. These include non-technical approaches such as conducting a risk assessment to identify areas of vulnerability, implementing a comprehensive cybersecurity policy, obtaining appropriate cybersecurity insurance coverage, and technical measures such as firewall protection, user education, and software vulnerability patching. Such tactics rely heavily on ransomware insurance, which provides monetary security and assistance for incident responses. The findings show that, while technological solutions are essential for efficient ransomware attack mitigation, they should be accompanied by strong insurance plans created to offer financial security in the event of an attack using static and dynamic analysis detection techniques. This article provides a thorough overview of the complexities of ransomware insurance strategies by synthesizing opinions from industry experts, legal viewpoints, and cybersecurity professionals. To reduce their exposure to potential crippling losses due to successful breaches, organizations must take proactive steps to defend themselves against the constantly evolving threat of ransomware by utilizing both technical and non-technical measures, including adequate cyber security insurance with machine learning techniques.

Keywords: Ransomware Insurance, Cybersecurity, Risk Management, Organization, Prevention, Machine Learning

Introduction

Ransomware was brought back into the limelight in 2017 with the broad and well reported WannaCry outbreak (Chang et al., 2019). This assault highlighted the magnitude of ransomware profitability as well as its potential destruction. Chaos and panic, but not financial gain, were the primary drivers of the WannaCry assault. Despite the low ransom demand of only $300, the resulting financial harm was predicted to be in the $4 billion range. Numerous ransomware assaults and variations have emerged in this regard. The COVID-19 epidemic has also been largely to blamed for the rise of recent cyberattacks (Detection et al., 2023). Employees' susceptibility to phishing emails increased as businesses adopted the remote work paradigm, creating security weaknesses in the organization's defense against cyber-attacks.

The proliferation of ransomware attacks has become a pressing issue in the field of cybersecurity, causing substantial financial losses and disruptions in various industries. Ransomware is a form of malicious software that encrypts valuable data on victims' systems, rendering it inaccessible until a ransom is paid to the attackers (Sarker et al., 2020). The exponential growth in the sophistication and frequency of ransomware attacks necessitates the development of effective pre-encryption detection approaches to identify and mitigate these threats before irreparable damage can be achieved. This study aims to provide a comprehensive understanding of Cybersecurity Risk Management with a Focus on Ransomware Insurance Strategies and approaches that are crucial for the early identification and mitigation of ransomware attacks in businesses, minimizing damage and financial losses. They enable initiative-taking incident responses, reduce downtime, and safeguard sensitive information from encryption and potential data breaches. By strengthening cybersecurity defenses and staying ahead of evolving ransomware threats, organizations can protect their systems and data and maintain operational continuity focusing on their taxonomy and research directions. By examining the existing literature and studies in the field, we seek to analyze the current state of knowledge, identify gaps, and propose future research directions. First, we present techniques including static and dynamic malware analysis, machine learning, anomaly detection, and signature-based detection. Thus, we aim to establish a conceptual model for ransomware detection that enables a structured comparison and evaluation of various approaches. Next, analyzed cybersecurity risk management, highlighting its strengths, prevention, and performance in different scenarios. This evaluation is based on observed studies, existing ransomware detection results, and real-world case studies, providing valuable insights into the efficacy of different detection approaches. Moreover, we explored emerging research directions in the field of ransomware detection. These include the integration of artificial intelligence (AI) techniques, such as deep learning and natural language processing, to enhance detection accuracy and speed. The malicious actor employs several strategies to acquire the capacity to encrypt the victim's data in a targeted crypto-ransomware assault. Such methods develop, sharpening their focus (Davies et al., 2021) and employing focused no-noise attacks on networks. The capacity and aim of encrypting victims' data so that only hostile actors can decrypt it upon the payment of the ransom distinguishes cryptographic ransomware from malware, despite the shifting of technology and some tactics. The findings and insights presented herein can serve as a foundation for researchers,

practitioners, and policymakers to design and implement advanced defense mechanisms against ransomware attacks (It & Vita, 2021; Richardson & North, 2017).

The rest of the paper is structured as follows. In Section 2, we describe the related work, malware analysis, and various ransomware target sources the ransomware domain, prevention, and security standards. We discuss the development of the research methodology for ransomware, in Section 3. Finally, we conclude with a summary in Section 4.

Literature Review

Cybersecurity has recently emerged as one of the biggest challenges for organizations. The Internet of Things (IoT) connects all individuals and organizations around the world with each other, making them more vulnerable to cyber-attacks. Cyber threats and attacks are not only limited to personal information, but also to data stored on organizational networks, cloud platforms, insider attacks, data breaches, financial data, and attacks on strategic resources. The international standards for information security, such as ISO/IEC 27000:2014, SNI ISO/IEC 27001:2013, and SNI ISO/IEC 27002:2013, can be used to develop information security management systems for organizations (Bhardwaj, 2019; Yaqoob et al., 2017). The study finds that I4.0 has not fully implemented measures for cyber risks, as recommended by leading cybersecurity frameworks. Currently, RiskLens and Cyberwar are the two primary quantitative cyber risk models. There is a consistent lack of disaster and recovery planning in all I4.0 initiatives. New emerging risks make it imperative to emphasize recovery planning for I4.0 implementation of (It & Vita, 2021). Ransomware attacks that can propagate this ability are the most dangerous. Figure 1 describes the role of Cybersecurity in Industry 4.0, Cybersecurity is being used as a core pillar for data protecting pcs, servers, mobile devices, electronic systems, networks, and data from malicious attacks, cyber security platform needs to manage and track cybercrime.

Companies increasingly depend on cyber security professionals to identify dangers and protect sensitive data such as data breaches, hacking, and cybercrime to reach new heights. With a Compound Annual Growth Rate (CAGR) of 9.7% from 2021 to 2026, the cyber security market is predicted to increase from $217 billion in 2021 to $345 billion by 2026 (Patel & Tailor, 2020).

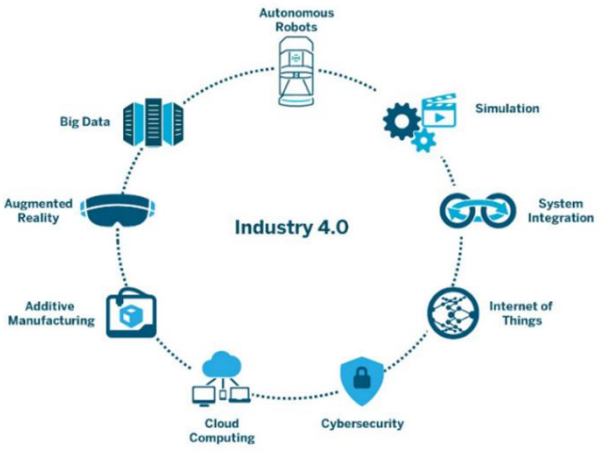

Figure 1. Industry 4.0 (Industrial Revolution INR)
(Source www.aethon.com)

Malware Analysis

Malware analysis is the process of analyzing dangerous software, sometimes known as "malware," to determine its features, patterns of behavior, and effects. This study provides researchers, defenders, and security professionals with the latest information on how the virus functions and how to lessen its impact. Malware analysis is essential for recognizing and thwarting online threats and for enhancing general cybersecurity procedures (Akhtar & Feng, 2022).

Static Analysis

Static analysis examines files without code execution to detect malicious intent. It helps identify infrastructure, libraries, or compressed files using technical indicators such as file names, hashes, and header data. Disassemblers and network analyzers can also be used to examine malware without active execution, thereby providing insights into their functionality (Malik et al., 2022).

Dynamic Analysis

Dynamic malware analysis uses a sandbox to execute malicious code, thereby providing enhanced visibility for security professionals and incident responders. This method eliminates the need for time-consuming reverse engineering and allows adversaries to evade detection by concealing the code within the sandbox until specific conditions are met. However, adversaries are aware of the existence of sandboxes and have developed techniques to avoid detection (Bayer et al., 2006).

The Evolution of Ransomware Evolution

A type of Trojan malware known as ransomware mostly affects computers using the Microsoft Windows operating system. Using social engineering and email attachments, ransomware spreads by masquerading as a regular file. When activated, the ransomware encrypts the data on the local network drive using an RSA open key and secret key that is encrypted and stored on its control server (Mansfield-Devine, 2016; Kharraz et al., 2015). Cybercriminals use ransomware, which is a type of malicious software, to prevent access to systems or data. Systems and data are hostage by the hostile cyber actor until the ransom is paid in Bitcoin.

Table 1
Comparative Analysis of Ransomware Insurance

Aspects	**Coverage Scope**	**Premium Costs**	**Coverage Limits**	**Exclusions**
Data Recovery	Extent of coverage for data recovery	Low/Moderate/High	Defined/Aggregate	Data loss due to non-ransomware incidents
Ransom Payment	Coverage for ransom payment	Moderate/High	Defined/Aggregate	Payments made without insurer's approval
Incident Response	Coverage for incident response	Moderate/High	Defined/Aggregate	Delays in reporting incidents

Business Interruption	Coverage for business interruption	Moderate/High	Defined/Aggregate	Delayed reporting of business interruption
Legal Support	Coverage for legal assistance	Low/Moderate/High	Defined/Aggregate	Legal actions due to non-compliance
Extortion Attempts	Coverage for extortion attempts	Low/Moderate/High	Defined/Aggregate	Extortion attempts unrelated to ransomware
Reputation Management	Coverage for reputation management	Low/Moderate/High	Defined/Aggregate	Negative PR unrelated to ransomware

Types of Ransomware

There are several types of ransomware, which are summarized in Table 2.

Table 2
Types of Ransomware

Ransomware Type	Description
Crypto Ransomware	Targets cryptocurrency wallets, steals credentials, or locks wallet for payment.
Locker Ransomware	Locks victim out of system, demands payment to restore access.
Scareware	Displays fake alerts, convinces payment for fake solutions.
Doxware	Encrypts files and threatens to leak sensitive data.
Ransomware as a Service	Criminals develop and sell ransomware to others.
Encrypting Ransomware	Encrypts files, demands payment for decryption. Examples: WannaCry, Ryuk.
Double Extortion Ransomware	Encrypts files, steals data, threatens data leak for payment.
Mobile Ransomware	Targets mobile devices, locks, or encrypts data for payment.

The Financial Effect of Ransomware

Ransomware assaults are now an increasing problem for commercial enterprises. By implementing strong IT infrastructure and efficient protection strategies, enterprises must be aware of the risks posed by ransomware and their effects. The primary driver of ransomware creation is monetary losses. Therefore, such malware infection costs millions of dollars, especially if weak safeguards are not used(Begovic et al., 2023).

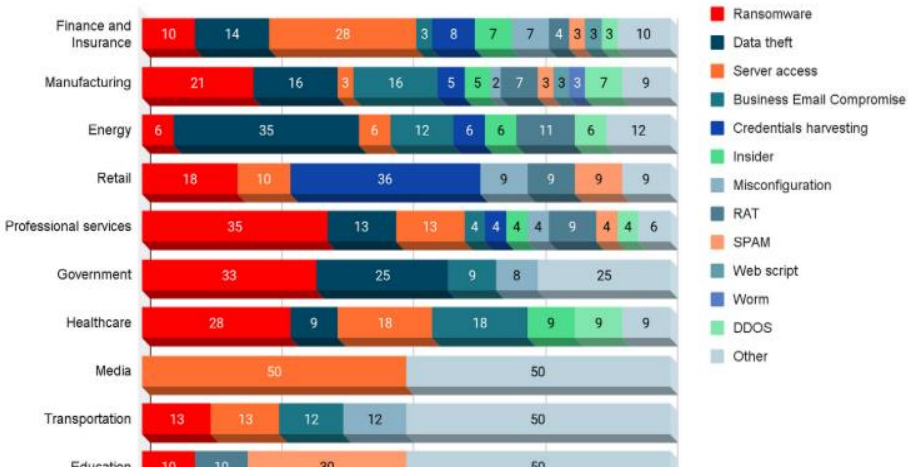

Figure 2. Attack Types per Industry
(Begovic et al., 2023)

Increased Ransom Demands and Incident Rates

Although ransomware has been present for some time, assaults have grown recently, both in terms of victims and attempted breaches (which, according to some predictions, will more than quadruple in 2021 to over 620 million). There were fewer ransomware assaults in the first few months of 2022, although this may have been caused by the disturbance in Ukraine and the sanctions that followed, which made it harder for hackers to organize their operations and demand ransom money. Some cybersecurity specialists predict that the current lull in ransomware activities will last only through Q2 2022 (Kalaimannan et al., 2017).

In recent years, the level of extortion demand has increased along with the number of ransomware assaults.

Table 3
Potential limitations for Ransomware Insurance Risk Mitigation

Pitfalls or Limitations	Description
False Sense of Security	Relying solely on insurance may create a false sense of security, leading to neglect of initiative-taking cybersecurity measures.
Financial Dependency	Over-reliance on insurance might make organizations financially dependent, inhibiting self-sustainability in dealing with ransomware threats.
Inadequate Coverage	Insurance policies may not provide adequate coverage for all aspects of a ransomware attack, leaving gaps in recovery or response expenses.
Evolving Ransomware Tactics	Rapidly evolving ransomware tactics and variants may outpace the coverage and response capabilities of insurance policies.
Exclusion Clauses	Insurance policies often have exclusion clauses related to specific circumstances, potentially limiting the coverage in certain scenarios.
Increased Premiums	Frequent ransomware claims can lead to increased premiums, making insurance a costly long-term mitigation strategy.
Time-Intensive Claim Process	The claims process can be time-consuming and complicated, delaying financial support needed for recovery after a ransomware attack.
Regulatory Compliance Implications	Ransom payments covered by insurance may have regulatory compliance implications, especially in industries with strict regulations regarding dealing with cybercriminals.

Early ransomware used simple data encryption methods, but cybercriminals have now adopted more advanced techniques. They now use up to four extortion methods to coerce victims into making payments. These methods can be combined in many ways, such as encrypting and stealing data and demanding a ransom to decrypt the information. The strategies, methods, and procedures (TTPs) of cybercriminals have also evolved to concentrate on network access footholds produced by other malware infections or software security flaws. They make use of weak places and single points of failure in the physical and digital supply chains of enterprises, particularly cloud-based apps, to spread malware and interfere with crucial infrastructure. They may even attack industrial control systems, to access their target systems before spreading the virus, as different methods used by ransomware attackers are shown in Figure 3 (Pain & Noordhoek, 2022).

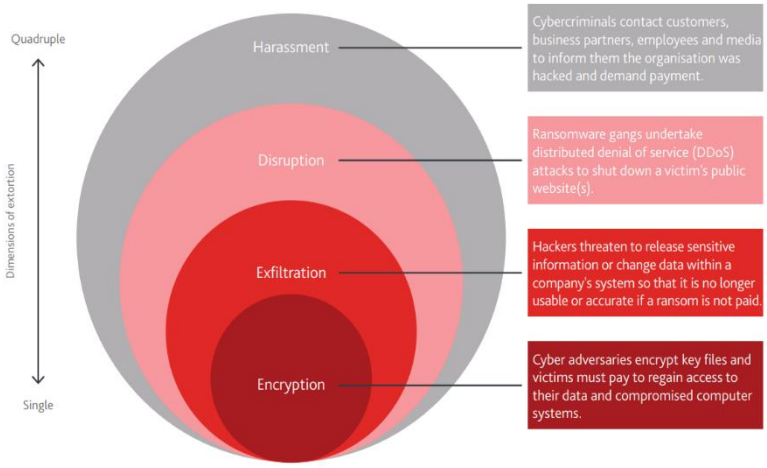

Figure 3. Extortion Methods Used by Ransomware Attackers
(Pain and Noordhoek, 2022)

a) Harassment

In recent years, ransomware attacks have become a serious cyber threat, causing significant financial losses and disruptions for people, organizations, and institutions. Beyond financial gain, these attacks may involve harassment to people or organizations to accomplish particular goals.

b) Disruption

Ransomware attacks have become increasingly frequent and sophisticated, disrupting a wide range of businesses, governments, and people. Such assaults cause major financial costs and brand harm by disrupting operations and encrypting crucial data.

c) Exfiltration

In addition to data encryption, ransomware operations increasingly involve data exfiltration, where they grab confidential data before it is encrypted. Organizations must consider data exfiltration in the context of ransomware.

d) Encryption

The critical data of an organization are frequently encrypted during ransomware attacks, making them unavailable until a ransom is paid.

Extortion demands have grown, and in Q4 2021, the average ransom payment jumped from USD 150,000 to USD 300,000. Some corporations pay millions in ransoms to restore their systems and data, which distorts the distribution of ransoms. A study found that mid-sized businesses paid an average ransom five times between 2020 and 2021.

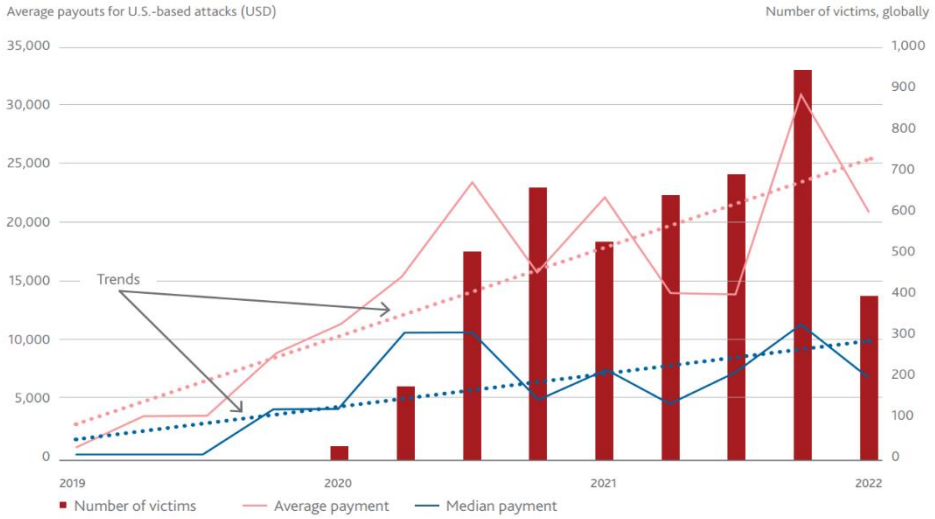

Figure 4. Ransomware Attack and Payment (Pain & Noordhoek, 2022)

Overview of Cyber Insurance

Industry professionals about the development of cyber insurance (and checking their recollections against the insurance industry literature), four broad generalizations became clear. There has been a long-term trend among insurers to move coverage for cyber risks out of their general-purpose liability and property insurance policies and into specialized cyber insurance policies, with the notable exception of extremely high value commercial property insurance policies, which frequently offer some data destruction and breach coverage, subject to comparably low sublimit. Cyber insurance products target specific risks and offer specific coverage with constrained limitations. Figure. 5 provides an illustration of these coverages by defining the coverage at the top, the type of coverage at the second level (first party, third party, or both), and the occurrence of coverage protection at the bottom. These regulations are designed to guard against various hazards, including online attacks, threats, and attacks (Baker & Shortland, 2023). Cyber insurance focuses on protecting against third-party risks, with policies including first-party coverage to offer customers and other parties' notices and services. By detecting compromised data and offering notice and privacy monitoring services, this coverage assists the covered firm in avoiding liabilities. First-party network security coverage also includes damage incurred in recouping from ransomware outbreaks and other network security breaches. Particularly when the breach is a component of a contemporary, "double extortion" ransomware assault, these losses can be ascribed to not just maintaining the covered organization but also avoiding or limiting liabilities to others.

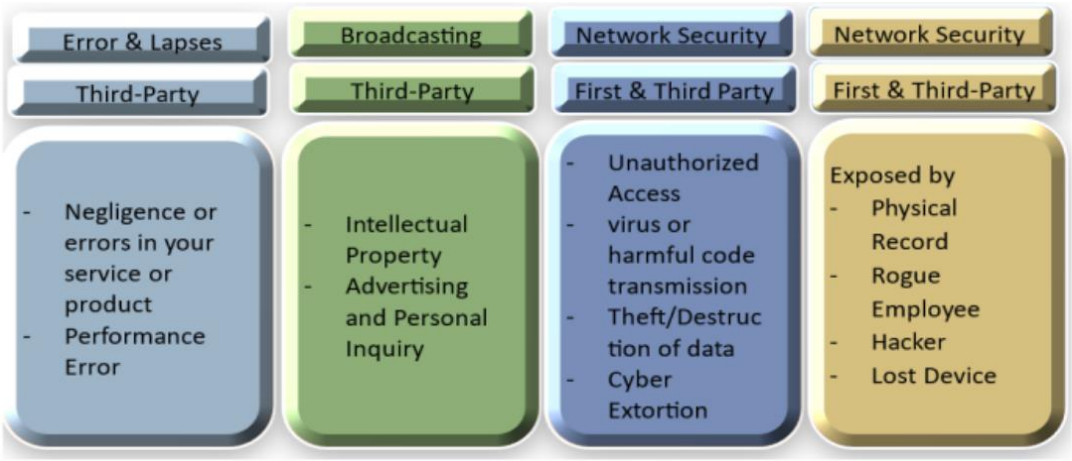

Figure 5. Cyber Insurance Polices

Cyber Protection For Ransomware

Data is encrypted by ransomware, a type of software that prohibits victims from accessing their files until ransom is paid. Over the past 30 years, this long-running trend has become more sophisticated. Cyber extortion was not a significant risk factor for insurers prior to 2013. However, as threats grew, potential victims and insurers took action to limit the likelihood that breaches would occur, boost resistance to extortion demands, enable amicable agreements, minimize collateral damage, and advocate for stronger law enforcement. The AIDS Trojan encrypted the computers of medical researchers in 1989, marking the first recorded case of ransomware (Moser et al., 2022). Their data were encrypted by Trojan, who also sought a USD 189 ransom. However, the payment procedure was complicated, and many people chose not to pay when security experts cracked the code. The threat of being monitored by legal authorities prevented subsequent extortionists from attempting to arrange payments through gift cards or premium telephone lines. Insurance had a beneficial effect as a result of this fear of cyber extortion, producing a larger premium income than insurance policies paid out (Baker & Shortland, 2023).

With professional-oriented hackers concentrating on obtaining and selling data, such as credit card information, or organizing botnets for denial-of-service assaults, cyber extortion first developed around 2005. The 2013 CryptoLocker ransomware outbreak was seen as a turning point because it brought ransomware to the public's notice (Patel et al., 2013).

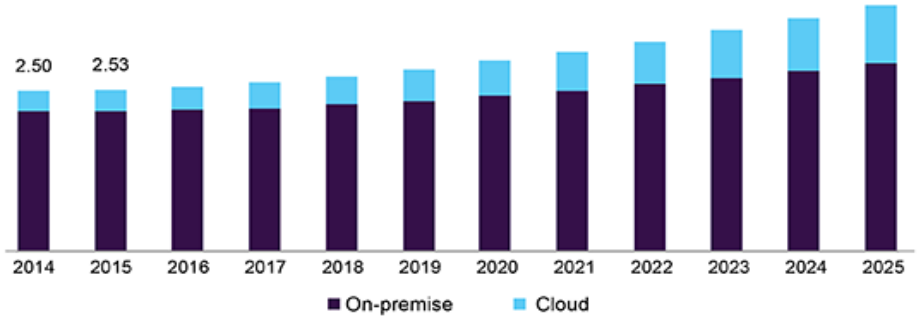

Figure 6. Software Market, by Development, 2014-2025 (by grand view research)

Cyber Insurance Management

The influence of cyber insurance extends beyond just covering ransom payments. Identifying recovery expenses separately from ransom offers a financial safety net that can reduce the urge to pay or give victims more time to think through their strategy for recovery or

negotiations. Access to ransomware response services may also assist victims to comprehend their alternatives.

Table 4
Cybersecurity Risk Management

Aspect	Description
Cybersecurity Risk	The potential of an event or incident to compromise information
Risk Assessment	Identifying, analyzing, and prioritizing potential risks
Threats	Potential events or actions that can exploit vulnerabilities
Impact	The consequences of a successful cyber attack
Vulnerabilities	Weaknesses or gaps in security that can be exploited by threats
Likelihood	The probability of a threat exploiting a vulnerability
Risk Calculation	Determining the level of risk based on impact and likelihood
Risk Mitigation	Implementing measures to reduce risk exposure
Controls	Safeguards and countermeasures to prevent, detect, or respond
Residual Risk	Remaining risk level after applying mitigations
Risk Monitoring	Continuously assessing, adjusting, and updating risk management
Incident Response	Preparing and responding to actual cyber incidents
Policy Framework	Establishing guidelines and protocols for risk management
Training & Education	Ensuring staff understand risks and proper security practices

Affecting and Target Selection

Several participants claimed that ransomware developers and their allies intentionally target businesses that have cyber insurance. These evaluations are based in part on conversations between cyber threat intelligence analysts and ransomware developers. For instance, a well-known ransomware operator connected to REvil once referred to cyber insurance victims as "one of the tastiest morsels" in a 2021 interview. The likelihood that ransomware operators and affiliates will utilize stolen information on policyholders to direct future operations has increased because of successful ransomware attacks against insurance firms. Understanding how ransomware affiliates enter organizations and the reasons for their victim prioritization are crucial for evaluating these claims. Affiliates of ransomware either gain access to businesses directly or make use of specialized access brokers active in the cybercriminal economy. In either scenario, opportunistic approaches or procedures are frequently used to compromise organizations. This may contain:

- Phishing campaigns
- Scanning for RDP instances
- Exploiting Vulnerability in internet-facing IT infrastructure

Table 5
Ransomware Insurance Strategies

Strategy	Description
Incident Response Coverage	Provides financial support for expenses related to managing a ransomware incident, including forensics, legal, notification, and crisis management costs.
Ransom Payment Coverage	Covers the ransom payment to cybercriminals, facilitating a faster resolution of the ransomware attack and potential recovery of encrypted data.
Business Interruption Coverage	Offers compensation for lost income and extra expenses incurred due to business interruption resulting from a ransomware attack.
Data Restoration and Recovery	Assists in covering the costs associated with data recovery, restoration, and system reconstruction after a successful ransomware attack.
Cyber Extortion Coverage	Provides coverage for threats other than data encryption, such as threats to expose sensitive data or launch a distributed denial-of-service (DDoS) attack.
Reputational Damage Coverage	Aids in managing and restoring the organization's reputation following a ransomware incident by covering PR and communication expenses.
Third-Party Liability Coverage	Protects against claims and legal expenses arising from third parties impacted by a ransomware incident, such as customers or business partners.
Cybersecurity Consultation Services	Offers access to cybersecurity experts and consultants to help improve the organization's cybersecurity posture and incident response capabilities.
Phishing and Social Engineering Coverage	Covers losses resulting from phishing attacks and social engineering schemes that lead to a ransomware incident.

Prevent Ransomware in Business Organization

- Regularly check user accounts, especially remote monitoring and managing (RMM) accounts that are visible to the public.
- Update endpoints, operating systems, applications, and software.
- Ensure that backups are safe and that they are unplugged from the network after each backup session.
- Watch network traffic coming in and going out; create data exfiltration alarms.
- Implement least privilege for file, directory, and network share permission.
- Inform staff members on ransomware methods and defense mechanisms, such as how to spot phishing emails and react to breaches.
- Use two-factor authentication for user logins, opting to receive SMS messages instead of emails in response to potential actor control of victim email accounts.

- Use risk assessments to classify data according to its sensitivity and worth.

Figure 7. Ransomware Prevention Strategy

Research Methodology

In this section, we outline the research methodology for the proposed detection against ransomware detection aimed at cybersecurity risk. Employing a mixed-methods strategy, core research methodologies, such as structured interviews and survey questionnaires, were utilized as tools for gathering and validating data in this research endeavor. Initially, structured interviews were conducted to identify the foundational factors and insurance measures.

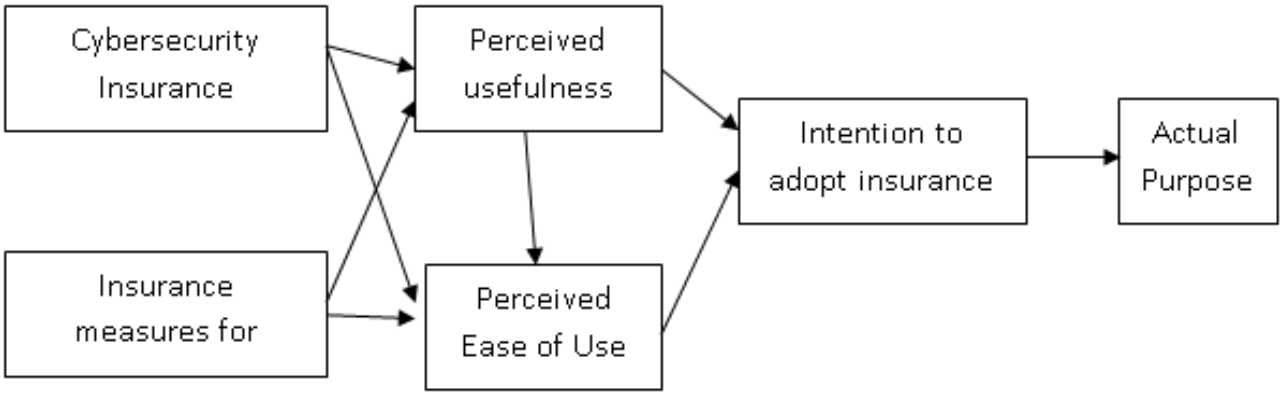

Figure 8. Research Methodology

Above illustrates progressively the stages outlined in the direction of this article. Each of the phases has activities to be carried out simultaneously.

Table 6
Respondent Analysis for Ransomware Insurance

No	Statements	Strongly Agree	Agreed	Disagree	Strongly disagree
1	Most respondents exhibited a moderate understanding of ransomware insurance, indicating a need for further awareness and education regarding its role in cybersecurity.	76 (75%)	20 (19%)	6 (6%)	
2	Cost was a significant consideration for most participants, highlighting the importance of affordable ransomware insurance solutions to encourage adoption.	66 (65%)	23 (22%)	11 (11%)	2 (2%)
3	Notably, many respondents recognized the value of ransomware insurance in augmenting their organization's overall cybersecurity posture and response capabilities.	45 (44%)	34 (33%)	19 (19%)	4 (4%)
4	A division was observed in respondent perspectives, with some driven by past ransomware incidents to explore insurance, while others were proactively evaluating its benefits.	81 (80%)	7 (7%)	6 (6%)	8 (7%)
5	Several participants expressed interest in comprehensive coverage and reputable insurance providers, emphasizing their careful consideration of several factors before selecting a ransomware insurance policy.	56 (55%)	32 (31%)	14 (14%)	
6	Concerns about the complexity of implementing a ransomware insurance strategy were evident among some respondents, underscoring the need for simplified and accessible insurance solutions.	78 (76%)	6 (6%)	18 (18%)	
7	Respondents' insights pointed towards a growing acknowledgment of ransomware insurance as an essential component in their risk management approach, highlighting an evolving mindset towards initiative-taking cybersecurity measures.	53 (52%)	43 (42%)	6 (6%)	

Conclusions

Ransomware insurance is a prime example of how insurance markets evolve over time, with insurers influencing the risk environment and reacting to shifts in other actors. To keep the

insurance markets feasible, it strikes a compromise between business and security. The main purpose of commercial insurance has always been to advance business, as determined by the goals of the covered organizations. Even when focusing on insurers' involvement in loss prevention, the literature on insurance as governance has never made any contrary claims. However, emphasizing the importance of business to insurance may help avoid erroneous conclusions. By giving consumers more assurance in the possibility of their companies, insurers can also advance security. To comply with the more restrictive definition of "security" implied by terms such as data and computer security, they participate in loss prevention and mitigation efforts, but do so in the enterprise, including their own, in service. Insurance companies can decide not to invest if they do not perceive a benefit for their own business. For instance, insurers concentrate on enterprises.

Acknowledgments

This research work is supported by the International Collaborative Research Fund (015ME0-326).

References

Akhtar, M. S., & Feng, T. (2022). Malware analysis and detection using machine learning algorithms. *Symmetry*, *14*(11). https://doi.org/10.3390/sym14112304

Baker, T., & Shortland, A. (2023). Insurance and enterprise: Cyber insurance for ransomware. *Geneva Papers on Risk and Insurance: Issues and Practice*, *48*(2), 275–299. https://doi.org/10.1057/s41288-022-00281-7

Bayer, U., Moser, A., Kruegel, C., & Kirda, E. (2006). Dynamic analysis of malicious code. *Journal in Computer Virology*, *2*(1), 67–77. https://doi.org/10.1007/s11416-006-0012-2

Begovic, K., Al-ali, A., & Malluhi, Q. (2023). Cryptographic ransomware encryption detection: Survey. *Computers & Security*, *132*(February 2022), 103349. https://doi.org/10.1016/j.cose.2023.103349

Bhardwaj, A. (2019). Ransomware: A rising threat of new age digital extortion. *Digital Currency: Breakthroughs in Research and Practice*, 313–339. https://doi.org/10.4018/978-1-5225-6201-6.ch017

Chang, H. Y., Lin, T. L., Hsu, T. F., Shen, Y. S., & Li, G. R. (2019). Implementation of ransomware prediction system based on weighted-KNN and real-time isolation architecture on SDN Networks. *2019 IEEE International Conference on Consumer Electronics - Taiwan, ICCE-TW 2019*, 4–5. https://doi.org/10.1109/ICCE-TW46550.2019.8991771

Davies, S. R., Macfarlane, R., & Buchanan, W. J. (2021). Differential area analysis for ransomware attack detection within mixed file datasets. *Computers and Security*, *108*, 102377. https://doi.org/10.1016/j.cose.2021.102377

Detection, A. I. M., Madhushalini, V., Raja, L., Song, W., Karanam, S., Xiao, Y., Qi, J., Dautenhahn, N., Meng, N., Danfeng, Yao, Begovic, K., Al-ali, A., Malluhi, Q., Jemal, M., Begovic, K., Al-ali, A., Malluhi, Q., Razaulla, S., … Cuppens, N. (2023). A proposed adaptive pre-encryption Crypto-Ransomware early detection model. *IEEE Access*, *10*(1), 3–8. https://doi.org/10.1109/CRC50527.2021.9392548

It, V., & Vita, A. (2021). *Ransomware study report*.

Kalaimannan, E., John, S. K., DuBose, T., & Pinto, A. (2017). Influences on ransomware's evolution and predictions for the future challenges. *Journal of Cyber Security Technology*, *1*(1), 23–31. https://doi.org/10.1080/23742917.2016.1252191

Kharraz, A., Robertson, W. K., Balzarotti, D., Bilge, L., & Kirda, E. (2015). Cutting the Gordian

Knot: A look under the hood of Ransomware Attacks. *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. https://api.semanticscholar.org/CorpusID:807905

Malik, K., Kumar, M., Sony, K. M., Mukhraiya, R., Girdhar, P., & Sharma, B. (2022). Static malware detection and analysis using machine learning methods. In *Advances and Applications in Mathematical Sciences* (Vol. 21, Issue 7).

Mansfield-Devine, S. (2016). Ransomware: Taking businesses hostage. *Network Security*, *2016*(10), 8–17. https://doi.org/https://doi.org/10.1016/S1353-4858(16)30096-4

Moser, A., Kruegel, C., Kirda, E., Wagener, G., State, R., Dulaunoy, A., Moskovitch, R., Elovici, Y., Rokach, L., Feher, C., Tzachar, N., Berger, E., Gitelman, M., Fernando, D. W., Komninos, N., Chen, T., Firdausi, I., Lim, C., Erwin, A., … Zafri, F. (2022). Cyber security threats and mitigation techniques for multifunctional devices. *Computers and Security*, *10*(1), 1–6. https://doi.org/10.1109/ICTAS.2018.8368745

Pain, D., & Noordhoek, D. (2022). *Ransomware: An insurance market perspective*. *July*, 1–4.

Patel, A., Taghavi, M., Bakhtiyari, K., & Celestino Júnior, J. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of Network and Computer Applications*, *36*(1), 25–41. https://doi.org/10.1016/j.jnca.2012.08.007

Patel, A., & Tailor, J. (2020). A malicious activity monitoring mechanism to detect and prevent ransomware. *Computer Fraud and Security*, *2020*(1), 14–19. https://doi.org/10.1016/S1361-3723(20)30009-9

Richardson, R., & North, M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10–21.

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, *7*(1). https://doi.org/10.1186/s40537-020-00318-5

Yaqoob, I., Ahmed, E., Rehman, M. H. ur, Ahmed, A. I. A., Al-garadi, M. A., Imran, M., & Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks*, *129*, 444–458. https://doi.org/10.1016/j.comnet.2017.09.003