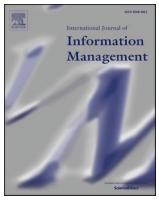
International Journal of Information Management 74 (2024) 102724



Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt





# A framework for cyber-risk insurance against ransomware: A mixed-method approach

Arunabha Mukhopadhyay *, Swati Jain

*Indian Institute of Management Lucknow, IIM Road, Prabandh Nagar, Mubarakpur, Lucknow 226013, Uttar Pradesh, India*

ARTICLE INFO

*Keywords:*
Cyber-risk insurance
Cybersecurity
Mixed method
Ransomware
Advanced persistent threat
Logistic regression

ABSTRACT

Hackers follow a standard cyber kill chain process and install ransomware payloads using phishing emails on firms belonging to critical industry, resulting in huge losses in revenue, reputation, and customer churn. This study uses a mixed-method explanatory approach to mitigate ransomware attacks. We present the quantitative Ransomware Risk Management Model (R2M2) based on protection motivation theory (PMT). The Ransomware Risk Assessment module based on the threat appraisal component of PMT and the National Institute of Standards and Technology (NIST) guidelines can help the chief information security officer (CISO) to assess the risk using predictive analytics techniques. The Ransomware Risk Quantification module uses collective risk modeling to compute the severity of a ransomware attack on an organization. The Ransomware Risk Mitigation module helps the CISO to minimize the probability and impact of a ransomware attack on their organization by (i) investing in perimeter security technologies and training to ensure prepare, deter, detect, restrain, recover, and review mitigation strategies, (ii) adopting the National Institue of Standards and Technology (NIST) Cybersecurity Framework to ensure business resilience, and (iii) mitigating the residual risk by investing in cyber-risk insurance. We validated the proposed method using a qualitative study by interviewing participants form firms affected by ransomware, managed security service providers, security consultants, and cyber-risk insurers.

## 1. Introduction

Ransomware is an advanced persistent threat (APT) that stealthily attacks the information system of an organization operating in the critical sector. This malware tends to encrypt essential files (*cryptographic ransomware*) and/or lockout users from the system (*locker ransomware*). As a result, the organization's operational activities come to a standstill, adversely affecting its revenue and reputation. These attackers demand high ransoms of cryptocurrencies (Laszka et al., 2017; Oz et al., 2022). Between 2019 and 2021, the number of ransomware attacks worldwide increased from 200 to 600. This upward trend is predicted to continue as hackers use more hybrid encryption algorithms and request ransom payments through cryptocurrencies (Oz et al., 2022). Between 2019 and 2021, the overall loss of revenue due to ransomware attacks increased from US$11.5 billion to US$20 billion. Consequently, the projected losses from ransomware attacks are anticipated to reach US$265 billion by 2031.

On November 23, 2022, a ransomware attack encrypted the data of the healthcare information system at the All India Institute of Medical Sciences (AIIMS), New Delhi, and a ransom of US$24.5 million was demanded. The healthcare delivery system at AIIMS came to a grinding halt for a week, which caused immense distress to patients and doctors. Similarly, a ransomware attack on May 31, 2022, exfiltrated the data from the Ministry of Finance of Costa Rica and US$15 million was demanded to restore the stolen information. Following this attack, the Costa Rican government declared a national emergency and suspended online government services.

Given these circumstances, the chief information security officer (CISO) of an organization should first conduct a detailed vulnerability assessment and then gather threat intelligence regarding the probable attack surfaces in the IT environment and attack vectors that a hacker may use as part of the cyber kill chain (CKC) (Lockheed, 2011) to launch a ransomware attack. Accordingly, the CISO must estimate the likelihood of a ransomware attack and its associated impact on the firm's operations. The CISO uses a heat matrix to visualize the above probability and impact and prioritizes mitigation strategies based on the NIST guidelines (NIST, 2018, 2022). Within this context, this study aims to use a mixed-method explanatory approach (Ballerini, Herhausen, &

* Corresponding author.
*E-mail address:* arunabha@iiml.ac.in (A. Mukhopadhyay).

https://doi.org/10.1016/j.ijinfomgt.2023.102724
Received 4 January 2023; Received in revised form 15 October 2023; Accepted 16 October 2023
Available online 3 November 2023
0268-4012/© 2023 Elsevier Ltd. All rights reserved.

Ferraris, 2023; Dwivedi et al., 2021; Kar & Dwivedi, 2020; Maier et al., 2023; Mikalef et al., 2019; Wunderlich et al., 2019) to examine the following research questions:

**RQ1).** What is the probability of correctly identifying a ransomware attack?

**RQ2).** What are the expected financial losses to a business from a ransomware attack?

**RQ3).** What are the means of mitigating (i.e., preventing, deterring, detecting, restraining, recovering, and reviewing) the effects of ransomware attacks by investment in technology and cyber-risk insurance?

This study contributes to the extant literature by proposing the comprehensive Ransomware Risk Management Model (R2M2) that assesses, quantifies, and mitigates ransomware risk based on the concepts of threat appraisal and coping appraisal in protection motivation theory (PMT) (Boss et al., 2015; Li et al., 2019; Ou et al., 2022; Rogers, 1975a; Yoo et al., 2020). The model comprises of three modules: Ransomware Risk Assessment (RRA), Ransomware Risk Quantification (RRQ), and Ransomware Risk Mitigation (RRM). The RRA module, which is based on the threat appraisal concept of PMT (Boss et al., 2015), helps the CISO to assess the risk of a ransomware attack on the organization, considering (i) the organizational structure, (ii) technological factors, (iii) environmental vulnerability, and (iv) information security governance. Hypotheses are tested using generalized linear models such as logistic regression (LR) (Mukhopadhyay et al., 2019; Son et al., 2020). Thethe RRA module uses predictive analytics techniques, namely L, naïve Bayes (NB), and decision tree (DT), to assess the ransomware risk. LR outperforms the other classifiers in terms of assessing the likelihood of ransomware attacks. Thereafter, the RRQ module computes the expected severity of a ransomware attack based on the likelihood and impact of the cyber risk (Biswas et al., 2023, Biswas et al., 2022; Hossack et al., 1983; Sharma and Mukhopadhyay, 2023). Finally, the RRM module helps the CISO to visualize the cyber risk of an organization on a heat matrix. This module is based on rational choice theory (RCT) (Becker, 1990; Boss et al., 2015; McCarthy, 2002), Kleindorfer & Kunreuther (1999)) and the NIST Cybersecurity Framework (NIST, 2014b, 2018) and helps to prioritize mitigation strategies for the CISO in terms of the proportion of cyber risks to be accepted, reduced, or transferred.

The remainder of this paper is organized as follows. A literature review on ransomware risk assessment, quantification, and mitigation is provided in Section 2. Section 3 introduces the research model and the corresponding hypotheses. Section 4 describes the quantitative assessment while Section 5 states the qualitative study. Section 6 discusses the results of the study and their implications for academia and industry. Finally, Section 7 concludes the paper.

## 2. Literature review

Organizations that belong to critical industries, such as healthcare, oil, and gas are prone to ransomware attacks, which lead to data exfiltration and locking of computer systems. According to risk (Kleindorfer & Kunreuther, 1999; Kunreuther, 1997; Kunreuther & Heal, 2003) and the NIST Cybersecurity Framework (NIST, 2018), the CISO of such organizations needs to carry out regular risk assessments and quantification of the vulnerabilities in IT resources that can be exploited to generate a possible cyberattack on the organization (Jain & Mukhopadhyay, 2023). These CISOs must understand the attacker's behavior using a CKC (Lockheed, 2011) and quantify the expected loss that can occur due to downtime or reputational loss accordingly. Furthermore, as per PMT (Boss et al., 2015; Rogers, 1975b) and RCT (Boss et al., 2015), the CISO, who is a rational actor based on the risk-profile of the organization, strategizes the cyber-risk mitigation policy (transfer, accept, or reduce). Therefore, we divide our literature review into three sections: ransomware risk assessment, ransomware risk quantification, and ransomware risk mitigation. The first subsection provides a review of the antecedents that have been considered in previous studies to determine the likelihood of data breaches caused by ransomware. The following subsection discusses methods used to quantify the risk of ransomware attacks. The final subsection reviews the strategies adopted to mitigate ransomware risks.

### 2.1. Ransomware risk assessment (RRA)

Ransomware can effectively compromise the IT defense of an organization and encrypt important files to prevent its operations. Previous studies on ransomware have primarily focused on the identification and detection of malware using technical features such as dynamic link libraries, registry keys, file processes, and payloads (Connolly & Wall, 2019; Yuryna Connolly et al., 2020). Static (Baldwin & Dehghantanha, 2018; pp. 107–136; Zuhair et al., 2020; pp, 1009, 3210) and dynamic (Cohen & Nissim, 2018; Ramesh & Menen, 2020) analyses have been performed to detect ransomware attacks. Static analysis entails identifying ransomware by extracting structural inputs, such as file information or malware opcodes, instead of executing (Oz et al., 2022). In contrast, dynamic analysis involves executing a sample and examining its behavioral characteristics, such as host logs, I/O access, or network activity, to identify the ransomware (Oz et al., 2022). However, very few studies have considered factors other than the characteristics of ransomware binaries. The study of socio-technical factors is essential for understanding why any organization falls victim to such attacks (Samonas et al., 2020). Ransomwares are growing into targeted attacks (Stolk, 2022), which highlights the importance of adopting a socio-technological approach. Considering this gap in the research, this study investigates factors that have been explored in a limited number of studies concerning ransomware as well as those that are used in assessing the risk of data breaches in general. The following subsections provide a literature review of the likelihood of ransomware attacks based on (i) the organizational structure, (ii) technological factors, (iii) vulnerability assessment, and (iv) information security governance (Angst et al., 2017; Boss et al., 2015; Weixun Li et al., 2023).

#### 2.1.1. Organizational structure

The size of an organization plays an important role in its organizational structure (Arad et al., 1997), Management Information System success (Raymond, 1985), computer use (DeLone, 1981), investment in internal or external IT resources (Ein-Dor & Segev, 1978), the symbolic or substantive adoption of cybersecurity measures (Angst et al., 2017), and the severity of ransomware attacks (Yuryna Connolly et al., 2020), among others. The levels of "risk tolerance" and "regulatory requirements" (Samonas et al., 2020; Tsen et al., 2022) vary depending on the sector (healthcare, financial, education, public administration and defense, manufacturing, etc.) to which a firm belongs (ARAD et al., 1997). Large organizations in critical industries are prone to ransomware attacks because they can adversely impact the economy of a country.

#### 2.1.2. Technological factors

Researchers have identified digital intensity as a significant technological factor that determines the occurrence of data breaches (Schlackl et al., 2022). Digital intensity refers to the extent of digital technology usage across different levels of operational and strategic activities within an organization (Bharadwaj et al., 2013; Chanias et al., 2019). Kim and Kwon (2019) found that as the use of electronic health records increases in hospitals, the risk of cyberattacks also increases. This observation was also noted by McLeod and Dolezel (2018), who assessed the level of exposure of a healthcare firm by implementing Computerized Physician Order Entry systems. Another study reported that the odds of facing ransomware attacks also increases with higher digital intensity (Smith et al., 2021). However, if such organizations also tend to have trained CISOs to ensure compliance with governance, their probability of facing ransomware attacks is reduced. Moreover, if the IT

network is well segregated, the chances and impact of a data breach are reduced (Shu et al., 2017). Even if an attacker gains unauthorized access, network segmentation prevents the further spread of the breach (Conti et al., 2018). It appears that few studies have investigated the impact of digital intensity and network segmentation on the occurrence of ransomware attacks.

#### 2.1.3. Vulnerability assessment

According to NIST (2014a), the computing environment of a firm encompasses its IT architecture and organizational features. Potential vulnerabilities in software, hardware, and networks can increase or decrease depending on the environment in which they exist (FIRST, 2019). Therefore, previous studies have suggested that vulnerability assessment is a critical factor to consider (Schlackl et al., 2022) in determining the risk of a ransomware attack.

#### 2.1.4. Information security governance

Information security governance refers to the centralized deployment of information security across an organization, considering the technical, process, and human perspectives (Liu et al., 2020). Additionally, the COBIT19 and ITIL frameworks provide effective guidance for organizations regarding the implementation of security in their IT infrastructure by following IT security governance principles (COBIT, 2007; Meijer et al., 2013). These frameworks recommend implementing IT controls to reduce risk and enhance the resilience of a firm. The level of resilience in the environment determines the extent to which a firm is exposed to a cyberattack (Schlackl et al., 2022). However, previous studies have not considered the organizational structure, technology, vulnerabilities, and information security governance together to assess the risk of ransomware attacks.

### 2.2. Ransomware risk quantification (RRQ)

The literature includes several studies that have quantified the losses arising from ransomware attacks. Ochoa et al. (2021) proposed a model that considers the probability of a ransomware attack ($p$) occurring as an input to express the impact of a ransomware attack in monetary terms. McIntosh et al. (2022) stated that the losses incurred by ransomware attacks are based on the type and duration of the attack, the cyber resilience of the organization, and preparedness against the attack. Few studies have quantified the risk of ransomware (R) attacks. Therefore, weextend our study to non-ransomware (NR) cyberattacks, such as denial-of-service (DoS), system penetration, and unauthorized access, in critical sectors such as finance, consultancy, education, IT, and healthcare organizations, to understand the methods used to quantify losses. Biswas et al. (2022), Sharma and Mukhopadhyay (2022), Mukhopadhyay et al. (2019), and Das et al. (2019) used various predictive analysis techniques (both structured and unstructured) to quantify cyberattack losses. Table 1 summarizes the techniques used to quantify losses caused by cyberattacks by firms across various industries. Considering the risk quantification methodologies for diverse attack types in various sectors, this study concludes that the expected loss is the product of the probability of a ransomware attack multiplied by the loss it incurs.

### 2.3. Ransomware risk mitigation (RRM)

The aftermath of ransomware attacks has motivated authors to explore mitigation measures (McIntosh et al., 2022). The following subsections outline mitigation methods in terms of the movement of a ransomware attacker along the line of the CKC. A cybersecurity team can check the timeline of events to understand the current state of attack, damage, and severity and respond accordingly to stop or minimize further damage (CISA, 2022).

**Table 1**
Summary of cyber-risk quantification studies.

| Year | Authors | Sectors | Type of Attack | Method |
|---|---|---|---|---|
| 2022 | Meshkat & Miller | Space | NR | JPL 5 × 5 risk matrix |
| 2022 | Biswas et al. | online hacker forums | NR | Text Mining |
| 2022 | Sharma & Mukhopadhyay | Smart City | NR | SARIMA |
| 2020 | Zuhair, Selamat, & Krejcar | Portable platform | R | Probabilistic-based |
| 2021 | Ochoa et al. | BFSI | R | Quantitative |
| 2019 | Mukhopadhyay et. al | BFSI | NR | Logistic Regression |
| 2019 | Das et al. | Healthcare | NR | Markov |
| 2018 | Baldwin and Dehghantanha | Portable Apps platform | R | ML-Based |
| 2017 | Cohen and Nissim | Cloud computing | R | ML-Based |
| 2017 | Angst et al. | Healthcare | NR | Statistical |
| 2013 | Mukhopadhyay et. al | BFSI | NR | Copula |
| 2008 | Wang et. al | Generic | NR | ML-Based, Text-mining |

#### 2.3.1. CKC pre-exploit phases (reconnaissance, weaponization, and delivery)

Previous studies have suggested that it is best to stop a ransomware attack during the reconnaissance and weaponization phases of the CKC to neutralize the attacker (Akbanov et al., 2019; Al-Rimy et al., 2018; Brewer, 2016; Harrison et al., 2022; McIntosh et al., 2022). A ransomware attacker attempts to reconnoiter the IT assets to identify vulnerabilities that can be exploited (Muckin & Fitch, 2019). The CISO should know the organizational environment (NIST, 2022) using a vulnerability scan to identify the weak links in hardware or software and the external connections of information flow that serve as entry points for ransomware attackers (Ramesh & Menen, 2020). The initial vulnerability assessment and subsequent patching will help to deter attackers (Ramesh & Menen, 2020). Building defensive boundaries shields the organization from the sights of the attacker and establishes security controls (NIST, 2022). It is always preferable to encrypt information so that it becomes difficult for an attacker to understand (Brewer, 2016). However, if the attacker successfully moves to the next stage of ransomware delivery, training employees not to click links in phishing emails or content filtering will help to identify and block the delivery (Li et al., 2019; Souppaya & Scarfone, 2013; Wong et al., 2022). Backups further help to restore data if a ransomware attack occurs (Muhly et al., 2022).

#### 2.3.2. CKC exploit and post-exploit phases (exploitation, installation, C&C, and actions)

After successful delivery of the payload, the attacker attempts to exploit the vulnerabilities to move laterally inside the network of the victim and remain undetected. This infiltration can be stopped by an intrusion detection system (IDS), intrusion prevention system (IPS), antivirus, or next-generation firewall (Harrison et al., 2022; IBM Security, 2022; Ramesh & Menen, 2020). In the next stage, the intruder attempts to install the ransomware and establish contact with the command & control (C&C) to conduct a ransomware attack. At this point, the security information and event management (SIEM) technologies will help to monitor the IT systems for ransomware binaries and generate alarms to awaken the cybersecurity team (IBM, 2022). Finally, the attacker attempts to encrypt or exfiltrate the victim's information or lock the victim's machine. At this point, the mitigation strategy should be avoiding further spreading of the attack (Souppaya & Scarfone, 2013). This can be achieved by disconnecting compromised systems from the infected network, temporarily stopping the use of the infected

application, and suspending internet access (IBM Security, 2022; NIST, 2022). Sandboxing or virtualization of applications or operating systems can also help stop the spread (CISA, 2022). Employees, clients, and vendors should be informed about the ransomware attack (Akbanov et al., 2019; Souppaya & Scarfone, 2013; Young, 2021). Later, business operations can be resumed with backed-up data (Baek et al., 2021; Chen et al., 2021; NIST, 2022; Straub & Welke, 1998). The systems or services that have been temporarily suspended because of ransomware infection can be restored (Muhly et al., 2022; Thakur et al., 2021). Most importantly, learning from the incident should be inculcated in the overall process of ransomware risk management, such as updating deterrence mechanisms (Baek et al., 2021; NIST, 2022). Prior research has suggested that organizations should quickly manage lost reputations or business relations (Muhly et al., 2022; NIST, 2022). Table 2 summarizes the ransomware attack mitigation methods proposed by previous researchers.

## 3. Research design

We adopted a mixed-method approach to explore the above research questions. This explanatory approach seeks answers to research questions through quantitative data (Ballerini et al., 2023; Dwivedi et al., 2021; Kar & Dwivedi, 2020; Maier et al., 2023; Mikalef et al., 2019; Wunderlich et al., 2019). The quantitative study considered the significant factors behind ransomware attack risk, guided by previous literature. Subsequently, we conducted a qualitative study using semi-structured interviews to gain a deeper understanding of the findings of the quantitative study. In the qualitative study, we focused on organizations that had experienced cyberattacks, as well as firms and consultants that provided the organizations with technological solutions and cyber-risk insurers. The perspectives and opinions of experts at different levels helped us to understand the dynamics behind why certain factors play a key role in determining the ransomware attack risk in a firm.

## 4. Quantitative study

### 4.1. Hypothesis development

The proposed R2M2 is based on PMT, which consists of two components: threat appraisal (TA) and coping appraisal (CA) (Boss et al., 2015; Li et al., 2019; Rogers, 1975a). We assume that the CISO of an organization is risk averse and such an individual will exhibit higher vigilance, appraise potential threats, and cope with the cyberattack situation (Kahane et al., 1988; Mukhopadhyay et al., 2019). Based on the TA component of PMT and the NIST guidelines, the RR module helps a CISO to assess the risk based on sociotechnical factors. These factors are considered because the risk of a ransomware attack does not depend solely on the technology that is implemented within an organization. It is also influenced by the culture, governance, and training provided to the employees of an organization (Wong et al., 2022). Next, the RRQ module computes the severity of a ransomware attack (R) on the organization (NIST, 2014b).

Similarly, based on the CA component of PMT, as well as RCT (Becker, 1990; Boss et al., 2015; McCarthy, 2002), trade-off theory (Campbell & Kelly, 1994), and conservation of resources (COR) theory (Hobfoll et al., 2000), the RRM module helps the CISO to minimize the probability and impact of the ransomware attack on their organization by (i) investing in perimeter security technologies (such as firewalls, IDSs, and antivirus) and training to ensure prepare, deter, detect, restrain, recover, and review (PDDRRR) mitigation strategies, (ii) adopting the NIST Cybersecurity Framework to ensure business resilience, and (iii) mitigating the residual risk by investing in cyber-risk insurance products (Mukhopadhyay et al., 2013). Fig. 1 depicts the proposed R2M2 model.

Table 3 summarizes the constructs used in the R2M2 model and their support in the literature.

#### 4.1.1. RRA

*4.1.1.1. Organizational structure.* According to the CKC model shown in Fig. 2 (NIST, 2014b), an attacker initially carries out reconnaissance to assess the potential benefits in terms of ransom (Oz et al., 2022) that they could gain from targeting an organization (NIST, 2022; Souppaya & Scarfone, 2013). Larger organizations, although better equipped with security technologies (Angst et al., 2017; Dalton et al., 1980; McLeod & Dolezel, 2018; Schlackl et al., 2022), would be severely impacted by a ransomware attack, as their IT-enabled supply chain may come to a standstill. To maintain seamless operations, a large organization will prefer to pay the ransom at times (Carroll & Stater, 2008). Therefore, this study proposes the following hypotheses:

**H1a.** : Larger organizations are more prone to ransomware attacks.

Firms in critical sectors (healthcare, finance, or public administration) ensure the security, integrity, and resilience of their operations by complying with strict regulatory guidelines (Jain, Mukhopadhyay &

**Table 2**
Summary of Ransomware Risk Mitigation Methods.

| | | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Pre-Exploitation** | Identify inventories | | | | | | | ✓ | | ✓ | ✓ | | | | |
| | Identify external connection | | | | | | | ✓ | | ✓ | ✓ | | | | |
| | Identify Information flow | | | | | | | ✓ | | ✓ | ✓ | | | | |
| | Defensive Architecture | | | | | | | | | ✓ | ✓ | | | | |
| | Fix vulnerabilities | | | | | | | | | | ✓ | | | | |
| | Encrypt & back up | | | ✓ | | | | | ✓ | | | | | | |
| | Train the staff | | | | | | | | | | | ✓ | | | |
| **During and Post Exploitation** | Scan continuously | | | | | ✓ | ✓ | | | | ✓ | | | | |
| | Raise alarms | | | | | ✓ | ✓ | | | | ✓ | | | | |
| | Block Payload | | | | | ✓ | ✓ | | | | ✓ | | | | |
| | Block C&C communication | | | | | ✓ | ✓ | | | | ✓ | | | | |
| | Disconnect network | | | | ✓ | | ✓ | | | ✓ | | ✓ | | | |
| | Shutdown Infected Service | | | | ✓ | | ✓ | | | ✓ | | ✓ | | | |
| | Suspend Internet Access | | | | ✓ | | ✓ | | | ✓ | | ✓ | | | |
| | Know Expected Move | | | | ✓ | | | | | | | ✓ | | | |
| | Communicate | ✓ | | | | | | | | | | ✓ | | | ✓ |
| | Resume operations | | ✓ | | | | | | | ✓ | | | ✓ | ✓ | |
| | Evaluate lessons | | ✓ | | | | | | | ✓ | | | | | |
| | Manage Reputation | | | | | | | | ✓ | ✓ | | | | | |

A: Akbanov et al. (2019); B: Baek et al. (2021); C: Brewer (2016); D: CISA (2022); E: Harrison et al. (2022); F: IBM Security (2022); G: Muckin & Fitch (2019); H: Muhly et al. (2022); I: NIST (2022); J: Ramesh & Menen (2020); K: Souppaya & Scarfone (2013); L: Straub & Welke (1998); M: Thakur et al. (2021); N: Young (2021)

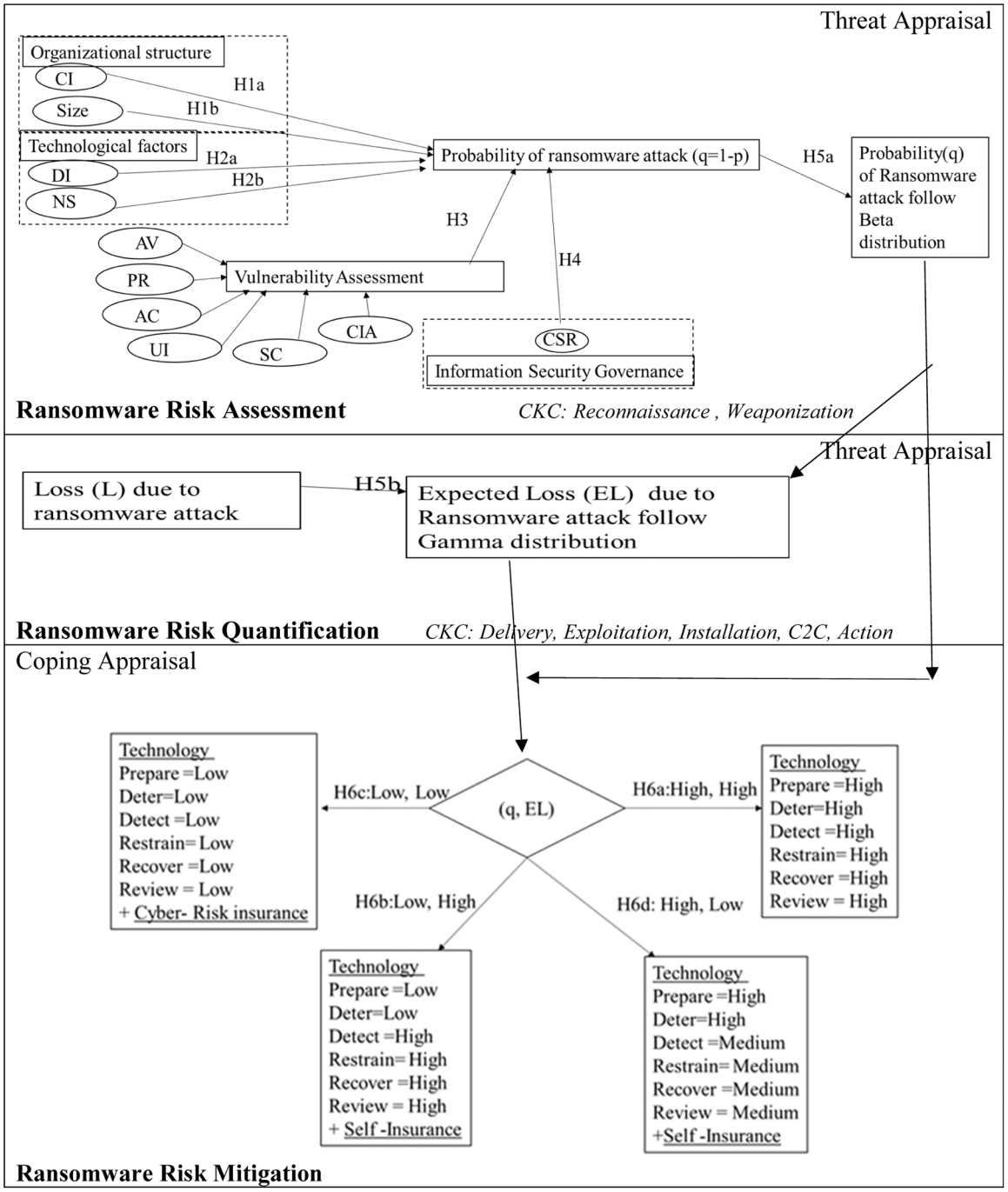



**Fig. 1. Proposed Model for Ransomware Risk Management** CI: Critical Industry; size: Organization Size; DI: Level of Digital Intensity; NS: Network Segmentation; AV: Attack Vector; PR: Privilege Required; AC: Attack Complexity; UI: User Interaction; SC: Scope; CIA: Confidentiality-Identity-Availability; CSR: Cyber-Security Role; EL= Expected Loss =q*L.

Jain, 2023; Samonas et al., 2020) for data protection, privacy, incident response, and contingency planning (Tripathi and Mukhopadhyay, 2022; Ballerini et al., 2023; Patel, Graham, & Ralston, 2008). This ensures operational continuity and maintains public trust and confidence in the ability of the firm to safeguard critical infrastructure and sensitive information (Samonas et al., 2020; Tsen et al., 2022). As indicated in Fig. 2, smart attackers choose to deliver weaponized APT tools such as ransomware to the servers of these firms to exfiltrate or encrypt sensitive data, disrupt essential services, and endanger the safety of citizens (ARAD et al., 1997). If these firms in critical sectors are impacted, the entire economy of a country may come to a grinding halt. Therefore, hackers have a greater chance of extracting ransoms from these firms. Thus, we hypothesize the following:

**H1b.** : Organizations belonging to critical industries are more prone to ransomware attacks.

*4.1.1.2. Technological factors.* Digital intensity indicates the degree of digitalization within a firm (Bharadwaj et al., 2013; Chanias et al., 2019). If an organization uses e-commerce as an important channel for revenue generation, customers and suppliers can use the internet to access customer relationship management (CRM) and supply chain management software. As shown in Fig. 2, a hacker can masquerade as a legitimate user and drop potential ransomware malware (Connolly &

**Table 3**
References of constructs used in the model R2M2.

| Modules | Variables | | Authors |
|---|---|---|---|
| | Organizational Structure | size | Schlackl et al. (2022); Kamiya et al., 2021;Yuryna Connolly et al. (2020);McLeod & Dolezel (2018); Angst et al. (2017); Arghandeh et al., 2016; Aoyama et al., 2015; ARAD et al. (1997);Raymond (1985);DeLone (1981);Dalton et al. (1980);Ein-Dor & Segev (1978); |
| | | CI | Tsen et al. (2022);Schlackl et al. (2022);Samonas et al. (2020); ARAD et al. (1997); |
| | Technological Factors | DI | Schlackl et al. (2022);Smith et al. (2021); Weill & Woerner, 2018; McLeod & Dolezel (2018) |
| | | NS | Schlackl et al. (2022); Carias et al., 2018;Shu et al. (2017) |
| | Vulnerability Assessment (EVSS) | AV, PR, AC, UI, SC, CIA | NIST (2022);Schlackl et al. (2022);FIRST (2019); |
| | Information Security Governance | CSR | Schlackl et al. (2022);Liu et al. (2020);Meijer et al. (2013); Bodeau et al. (2010);Bowen & Wilson (2006);COBIT (2007); |
| RRQ | Misclassification Rate | q | Sharma & Mukhopadhyay (2022);Zuhair et al., 2020, pp. 10093210;Ramesh & Menen (2020);Zhang et al. (2019); Baldwin & Dehghantanha, 2018, pp. 107–136;Cohen & Nissim (2018); |
| | Expected Losses | EL | Meshkat & Miller, 2022;Biswas et al. (2022);Zuhair, Selamat, and Krejcar, 2020, pp. 10093210; |
| RRM | Mitigation strategies | PDDRRR | McIntosh et al. (2022);CISA (2022);Harrison et al. (2022); Muhly et al. (2022);McIntosh et al. (2022);NIST (2022);Baek et al. (2021);Chen et al. (2021); Akbanov et al. (2019);Al-Rimy et al. (2018);NIST (2018);Brewer (2016);Mukhopadhyay et al. (2013);Souppaya & Scarfone (2013); Gordon et. al, 2003b; Straub & Welke (1998) |

CI: Critical Industry; size: Organization Size; DI: Digital Intensity; NS: Network Segmentation; AV: Attack Vector; PR: Privilege Required; AC: Attack Complexity; UI: User Interaction; SC: Scope; CIA: Confidentiality-Identity-Availability; CSR: Cyber-Security Role; q = (1-p); PDDRRR: Prepare, Deter, Detect, Restrain, Recover, Review

Wall, 2019). For example, a hospital that allows online patient booking facilities would come to a standstill if the ransomware locks its CRM or encrypts its database and demands a ransom in exchange (Al-Rimy et al., 2018; Zhang et al., 2019). Hence, we hypothesize the following:

**H2a**. Higher digital intensity leads to an increased probability of ransomware attacks.

As shown in Fig. 2, after the successful delivery of the payload in the digital systems, a hacker will remotely attempt to exploit the vulnerabilities and communicate the same to the C&C center (FIRST, 2019; McIntosh et al., 2022). A CISO (i) compartmentalizes the larger network into a smaller virtual LAN, (ii) separates critical applications or servers from the internet, and (iii) restricts the movement of the ransomware from a compromised system to an uninfected critical system (Conti et al., 2018; Mos & Chowdhury, 2020). Sandboxing or virtualization of applications or operating systems also helps to stop the spread of ransomware (CISA, 2022). Hence, we hypothesize the following:

**H2b**. The segmentation of the IT network will block ransomware attacks.

*4.1.1.3. Vulnerability assessment.* As shown in Fig. 2, an external hacker exploits the vulnerabilities (Schlackl et al., 2022) in a digital platform by resorting to attack vectors such as social engineering to carry out a confidence–integrity–availability (CIA) breach (FIRST, 2019; Zhuang et al., 2020). For instance, a hacker can trick a customer into clicking on a phishing email that can exploit vulnerabilities in the CRM software of a firm. The hacker intends to misuse the privilege of customers and employees (PR) (O'Kane et al., 2018; Oz et al., 2022). Once a hacker obtains access to the CRM system, it delivers the payload to the target software or network. In most cases, the hacker does so without engaging the user (UI) and without changing the authorization rights (scope (SC)) of the vulnerable client portal or business rules, which in turn brings the supply chain management of the digital platform to a standstill, resulting in a huge loss of revenue, reputation, and customer churn (Almashhadani et al., 2019; Dargahi et al., 2019; Lockheed, 2011). Hence, the literature suggests that the CISO should know their organizational environment (NIST, 2022) well before the adversary does. Using the concepts of threat intelligence and the CKC (Lockheed, 2011), the CISO of an organization can reduce the vulnerability in the organization's environment. For instance, an organization that sets privileges as more restrictive (PR) is less exposed to the risk of a ransomware attack (Peters, 2017). FIRST (2019) defined the vulnerability score, which is platform and vendor agnostic, and considered the environmental conditions that increase and decrease the impact of such vulnerabilities on an organization. Based on this understanding, we hypothesize the following:

H3: Organizations with high environmental vulnerability scores are more likely to encounter ransomware attacks.

*4.1.1.4. Information security governance.* According to the coping appraisal component of PMT (Boss et al., 2015; Rogers, 1975a), the top leadership of an organization will attempt to reduce the likelihood of ransomware attacks. To achieve this, they implement an information security governance framework that is aligned with the strategic goals of the organization (Fazlida & Said, 2015; Weixun Li et al., 2023). This implementation incorporates cybersecurity controls and measures that are aimed at reducing the environmental vulnerability score (Schlackl et al., 2022) and, consequently, the probability of a ransomware attack (Bodeau et al., 2010; Bowen & Wilson, 2006). Therefore, we hypothesize the following:

**H4**. : Organizations that have implemented information security governance are less likely to experience ransomware attacks.

*4.1.1.5. Likelihood of a ransomware attack.* An intruder can install ransomware and threaten to exfiltrate or encrypt the information that is stored in the IT assets (Muckin & Fitch, 2019). The hacker claims a ransom in return for restoring the operations of the IT assets. As shown in Fig. 2, the CISO uses historical data from endpoint detection and response (EDR), extended detection and response (XDR), and SIEM to create a model for classifying the likelihood of a ransomware attack on a firm. Previous studies have noted that cyberattacks tend to follow a Weibull distribution (Hossack et al., 1983). This is because a small number of cyberattacks occur frequently. For example, DDoS attacks that send packets of moderate sizes to clog the network, are large in number, but large-sized packets causing DDoS attacks will be lower in number. Furthermore, the flexibility of the Weibull distribution allows it to accommodate various shapes, making it adaptable to a wide range of cyberattack scenarios (Wang et al., 2015). By adjusting the shape parameter, it is possible to model various characteristics of different cyberattack situations. The scale parameter corresponds to the position of the Weibull curve relative to the threshold, similar to how the mean influences the position of a normal curve (Hossack et al., 1983). Hence, we hypothesize the following:

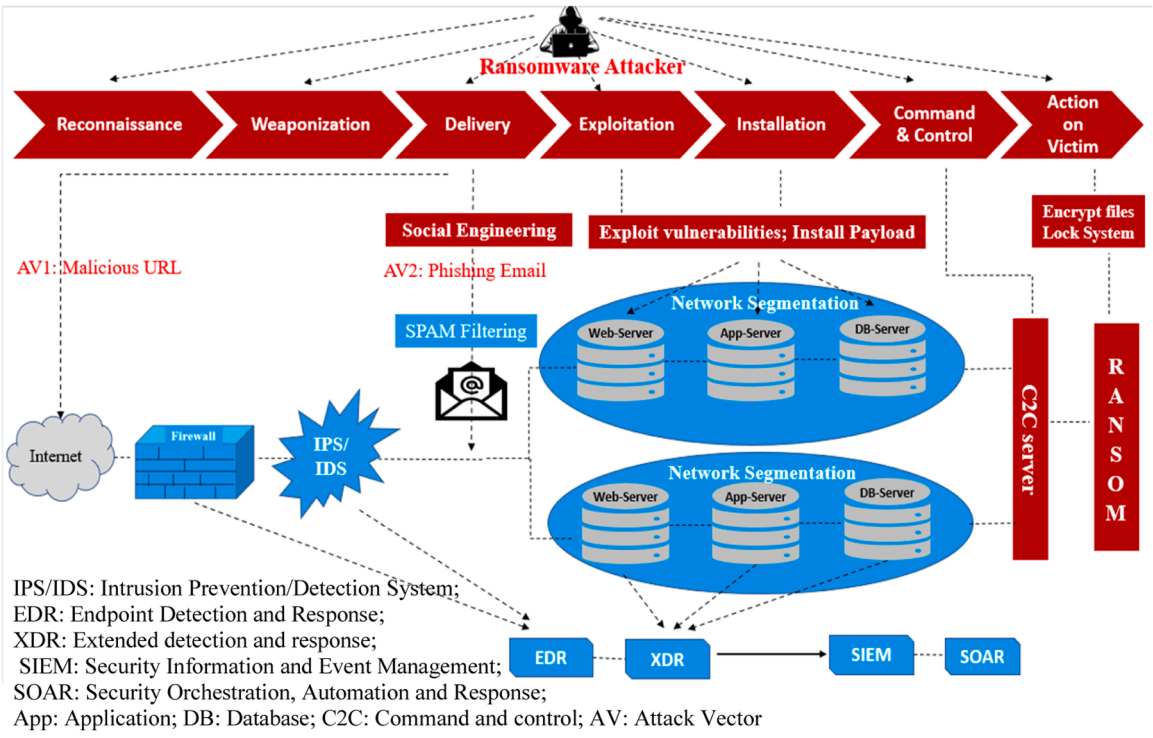



**Fig. 2. Ransomware Attacker's Move as per Cyber Kill Chain (CKC) Vs Cyber-security Team's Defense (**Red: Attacker's Move (CKC); Blue: Cyber-security Personnals' Defense).

**H5a**. : The probability of occurrence of ransomware and non-ransomware attacks on an organization tends to follow a Weibull distribution.

#### 4.1.2. RRQ

If the operations of an organization belonging to a critical industry (healthcare, financial services, or supply chain) are stalled, this leads to immense monetary losses (Biswas et al., 2022). The RRQ module considers such losses (L), along with the risk probability (p) computed in the RRA module, to calculate the severity of the attack in terms of the estimated losses (EL). The losses arising from cyberattacks follow a long-tail gamma distribution (Mukhopadhyay et al., 2019; Dutta & Perry, 2006). It is noted that losses due to ransomware generally tend to be low in magnitude, but some, such as WannaCry, which impacted the National Health Services (NHS) and spread very quickly across the globe, had a high impact of US$4 billion globally (Hossack et al., 1983; Wang et al., 2015). Hence, we hypothesize the following:

**H5b**. : The expected losses arising from ransomware and non-ransomware attacks follow a gamma distribution.

#### 4.1.3. RRM

Finally, the RRM module provides recommendations for mitigating the losses resulting from a ransomware attack on an organization. According to the CA of PMT theory, the CISO of a firm responds to fear appeals of cyber threats by taking appropriate mitigating actions (Boss et al., 2015). The RRM module assists the CISO in determining whether to absorb, transfer, or reduce the cyber risk resulting from the ransomware attack. The model uses the NIST Cybersecurity Framework (NIST, 2018) and the mitigation strategies suggested by Straub and Welke (1998) to guide the decision-making process. These methods are divided into the six phases of PDDRRR, as shown in Table 4. The prepare and deter phases cover the pre-exploitation activities. The detect, restrain, recover, and post-incident review phases include the post-exploitation mitigation methods.

Initially, the CISO should prepare the organization against ransomware attacks by identifying the most critical inventory of the IT assets, their internal and external connections, and the information flow route to neutralize the CKC. Employees should be trained to identify and prevent attacks by recognizing phishing emails and avoiding clicking unknown links. Data encryption and remote backups are important for protection and recovery in later stages. Frequent dry runs of incident responses are conducted to develop alertness and awareness among employees and other stakeholders to combat ransomware attacks. Following preparation, the CISO should attempt to detect ransomware attacks by ensuring perimeter security using antivirus, IDSs/IPSs, and new-generation firewalls and by performing vulnerability assessment and penetration testing to analyze IT assets or network vulnerabilities.

Even with a robust deterrence mechanism, if the ransomware enters an IT system, detection methodologies are crucial for quickly detecting and stopping it. Regular monitoring of the system, ensuring cyber-hygiene (Wong et al., 2022), detecting unidentified ransomware, raising alerts, and blocking payload or C&C communications are important steps. If an attack cannot be stopped, the CISO should focus on restraining it and preventing its further spread. This involves quarantining infected files or systems, disabling infected services, and

**Table 4**
Technological interventions to mitigate ransomware risk.

| | | | |
|---|---|---|---|
| Prepare | Identify IT assets<br>Identify external network<br>Upskilling staff | Restrain | Quarantine infected files<br>Apply Threat Intelligence<br>Facilitate coordination |
| Deter | Vulnerability Assessment<br>Encrypt & back up<br>Perimeter security<br>Frequent dry runs | Recover<br><br>Review | Implement BCP / DRP<br>Restore system/services<br>Fix gaps in IRP<br>Manage Public Relations |
| Detect | Monitor & Alert<br>Block Payload<br>Block C&C communication | | |

BCP: Business Continuity Plan; DRP: Disaster Recovery Plan; IRP: Incident Response Plan

suspending internet connectivity. Additionally, leveraging threat intelligence mechanisms can help to mitigate the impact by analyzing the attack and anticipating the next move of the attacker. Effective communication and coordination among all stakeholders is required to beat attackers. If a firm faces losses, it should immediately seek to implement a business continuity plan (BCP) or disaster recovery (DR) plan, which is specifically designed for such contingencies, to recover from the losses. An infected system can be restored using backed-up data to ensure minimal disruption to business operations. Following an incident, it is important to conduct a post-incident analysis to identify shortcomings in the incident response plan. All phases of the ransomware risk mitigation strategy should be reviewed and updated as necessary. Additionally, the CISO should seek to compensate for lost reputation and public relations.

However, it is important to note that organizations face constraints in terms of time, money, and resources, as suggested by the COR theory (Gordon et al., 2003a). The decision of investments in different PDDRRR phases may vary depending on the risk-severity quadrant on the heat matrix to which the organization belongs, which is in line with the trade-off theory. For instance, organizations that face ransomware attacks (Q1) should invest a high proportion in deterrence activities with a low proportion in detection or restraint activities. Therefore, the model advises the CISO on the level of importance – high (H), medium (M), or low (L) – to be assigned to mitigation methods (PDDRRR), based on the location of the organization in the heat matrix (risk × severity).

The CISO of organizations in Q1 should focus on all aspects of the PDDRRR mitigation strategies to reduce the probability and severity of ransomware attacks. This is because cyber-insurance firms are unwilling to provide such organizations coverage against ransomware attacks (Muhly et al., 2022; Mukhopadhyay et al., 2013). Hence, we hypothesize the following:

**H6a**. : If an organization faces a high probability and high severity of a ransomware attack, the CISO tends to prioritize investments in cybersecurity technologies for PDDRRR.

When an organization in the Q2 quadrant of the heat matrix experiences a low probability of a ransomware attack, the CISO can focus less on the prepare and detection phases and more on the remaining PDDRRR phases. The CISO should devise an effective BCP and DR policy to restore the information systems and ensure business continuity. This will help to reduce the severity of ransomware attacks and, consequently, the firm will move from Q2 to Q3 in the heat matrix. Hence, we hypothesize the following:

**H6b**. : If an organization faces a low probability but high severity of a ransomware attack, the CISO tends to prioritize more security technology investment in the detect, restrain, recover, and review activities than the prevent and deter activities against the attack.

If a firm is in quadrant Q3, cyber insurers will not hesitate to provide cyber insurance. Hence, such organizations can invest in cyber-insurance policies to protect themselves against future losses from ransomware attacks. As the CISO has transferred the risk to cyber insurers, the focus on the PDDRRR will automatically be reduced. Hence, we hypothesize the following:

**H6c**. : If an organization faces a low probability and low severity of a ransomware attack, the CISO tends to invest more in cyber insurance than in PDDRRR mitigation strategies.

Organizations in quadrant Q4, where the probability of an attack is high but the severity of the attack is low, should focus more on the prepare and deter stages and can moderately focus on other PDDRRR stages. The CISOs of such firms should initially resort to self-insurance and inculcate technology interventions such as firewalls, antivirus, and IDPs/IPSs to build defensive architectures. Such measures will help to reduce the probability of ransomware attacks and, consequently, move the firm from Q4 to Q3. Hence, we propose the following hypothesis:

**H6d**. : If an organization faces a high probability but low severity of a ransomware attack, the CISO tends to prioritize more security technology investment in the prevent and deter activities than the detect, restrain, recover, and review activities against the attack.

**Table 5**
Summary statistics of data from 2004 to 2022 of n = 1473 organizations.

| Variables | Values | Count | Min* | Max* | Mean* | Std Dev* |
|---|---|---|---|---|---|---|
| **Critical Industry (CI)** | No | 604 | 0 | 89 | 27 | 25 |
| | Yes | 869 | 2 | 137 | 41 | 39 |
| **Organization size (Size)** | Small | 619 | 0 | 95 | 22 | 23 |
| | Large | 854 | 2 | 97 | 49 | 29 |
| **Digital Intensity (DI)** | Low | 732 | 0 | 86 | 27 | 25 |
| | High | 741 | 0 | 57 | 17 | 17 |
| **Network Segmentation (NS)** | No | 474 | 0 | 63 | 19 | 19 |
| | Yes | 999 | 1 | 161 | 51 | 47 |
| **Vulnerability Assessment (EVSS)** | | | | | | |
| *Attack vector (AV)* | Local | 279 | 0 | 39 | 8 | 13 |
| | Network | 1164 | 1 | 181 | 61 | 53 |
| | Physical | 30 | 0 | 5 | 2 | 1 |
| *Privileges Required (PR)* | High | 152 | 0 | 9 | 1 | 2 |
| | Low | 1321 | 1 | 221 | 73 | 60 |
| *Attack Complexity (AC)* | High | 22 | 0 | 8 | 2 | 2 |
| | Low | 1451 | 1 | 219 | 69 | 63 |
| *User Interaction (UI)* | None | 1098 | 1 | 177 | 59 | 54 |
| | Required | 375 | 0 | 45 | 12 | 12 |
| *Scope (SC)* | Changed | 1264 | 2 | 223 | 69 | 63 |
| | Not Changed | 209 | 0 | 7 | 2 | 1 |
| *Confidentiality-Integrity- Availability (CIA)* | Confidentiality | 1203 | 1 | 189 | 66 | 57 |
| | Integrity | 133 | 0 | 5 | 1 | 1 |
| | Availability | 137 | 0 | 34 | 7 | 8 |
| **Information Security Governance** | | | | | | |
| *Cyber-security Role (CSR)* | No | 1156 | 1 | 203 | 7 | 57 |
| | Yes | 317 | 1 | 19 | 8 | 61 |
| **Attack** | Non-Ransomware | 1207 | 1 | 188 | 65 | 55 |
| | Ransomware | 266 | 0 | 32 | 7 | 9 |
| **Losses (L)** | In Million US$ | 1473 | 32 | 4219 | 1254 | 797 |

* represents per year occurrence

### 4.2. Methodology and data

This study used data from the University of Queensland, Australia, to explore the cyber resilience of organizations (Tsen et al., 2020). The dataset consisted of various features of 1473 organizations belonging to the critical and non-critical sectors in Australia, the USA, Canada, and Japan and their associated breaches due to ransomware attacks from 2004 to 2022. The dataset included firms with varying digital intensity, organizational size, network segmentation, EVSS, and CSR. We referred to Statista for data on the average financial losses ($L_j$) (Statista, 2022) from 2004 to 2022, which are derived from cyber-crime cases reported by the Internet Crime Complaint Center (IC3), which is a part of the FBI. Table 5 summarizes the statistics of the data.

Table 6 shows the relationship between the dependent and independent variables.

#### 4.2.1. RRA

Previous researchers have commonly used the following algorithms to detect ransomware: the support vector machine (Baldwin & Dehghantanha, 2018, pp. 107–136), random forest (Cohen & Nissim, 2018; Zhang et al., 2019), DT (Zhang et al., 2019; Zuhair et al., 2020; pp, 1009, 3210), NB (Cohen & Nissim, 2018; Zhang et al., 2019; Zuhair et al., 2020; pp, 1009, 3210), and LR (Cohen & Nissim, 2018). Table 7 summarizes the various static and dynamic features that are considered to detect ransomware using different rule-based and machine-learning-based methods.

We initially tested the hypotheses using generalized linear models, such as LR in module M1, as shown in Eq. (1) (Agresti, 2002; McCullagh & Nelder, 1989; Mukhopadhyay et al., 2019; Son et al., 2020).

$$\mathrm{M1(LR)}: P(C = \text{Ransomware, Non-Ransomware}) = \frac{1}{(1+\exp^{-Z})} \cdots \quad (1)$$

$$Z = \beta_0 + \beta_1 *\mathrm{CI} + \beta_2 *\mathrm{Size} + \beta_3 *\mathrm{DI} + \beta_4 *\mathrm{NS} + \beta_5 *\mathrm{EVS} + \beta_6 *\mathrm{CSR}$$

Next, in our RRA module, we used predictive analytics techniques such as LR, NB, and DT in modules M1, M2, and M3, respectively, to assess the likelihood of ransomware attacks versus non-ransomware attacks. M1 uses LR, which is a special case of the generalized linear model that provides the probability of occurrence of each binary class (Son et al., 2020). LR is one of the most renowned and extensively employed predictive models in the literature (Bardhan et al., 2015; Ben-Assuli & Padman, 2020). The second classifier, M2, uses the NB classification technique to estimate the probability ($p$) of a ransomware attack. The NB classifier is a probabilistic classifier based on Bayes' theorem that assumes that the variables are independent of one another (Han et al., 2012). Finally, M3 uses the DT classification technique to generate rules to classify R and NR and to estimate the probability ($p$). The NB classifier is a probabilistic classifier based on Bayes' theorem that assumes that the variables are independent of one another. Similar to the NB algorithm, the DT algorithm is a supervised learning technique that is used to perform predictions (Ben-Assuli & Padman, 2020; Yahav et al., 2016). Previous studies have predicted the readmissions of patients with chronic diseases (Ben-Assuli & Padman, 2020), financial fraud (Abbasi et al., 2012) and false news on social media (Wei et al., 2022),

The dataset was divided into training and testing sets at a ratio of 70:30. The LR, NB, and DT classifiers were initially trained and then evaluated using the test dataset. A predictive model is gauged according to its performance on data instances that have not been encountered before and are found within a designated test dataset (Bardhan et al., 2015). The performance of the model was evaluated by computing the accuracy, F-score, precision and recall. This study assessed the risk and obtained the consequent posterior probabilities ($p_i$) of an attack being R or NR.

#### 4.2.2. RRQ

We calculate the severity of a ransomware attack by computing the *expected losses* ($EL_i$) (Biswas et al., 2022). The mathematical representation of the expected financial loss ($EL_i$), as shown in Eq. (2), is.

$$EL_i = q_i * L_j \quad (2)$$

where $q_i$ = misclassification rate = *1 - $p_i$*; $p_i$ = *posterior probabilities*; $L_j$ = losses in each year from 2004 to 2022; $EL_i$ = estimated loss for each organization; and i = organization in the dataset.

#### 4.2.3. RRM

Based on the likelihood of a ransomware attack and its severity, the RRM module creates a 2 × 2 (risk (q) × severity (EL)) heat matrix. Each data point is placed in one of the four quadrants (high-high, low-high, low-low, and high-low) of the heat matrix. This can help the CISO of an organization to decide whether to absorb, transfer, or reduce the cyber risk (Baskerville et al., 2008) related to a ransomware attack. The RRM module guides the CISO in prioritizing the proportion of investment in PDDRRR mitigation strategies based on a threshold of risk ($q_i$) and severity ($EL_i$). Each test data point is plotted on the heat matrix.

### 4.3. Results

This section describes the quantitative results obtained from the RRA, RRQ, and RRM experiments. Section 4.3.1 describes the likelihood of a ransomware attack, Section 4.3.2 presents the expected losses due to ransomware attack, and Section 4.3.3 explains the placement of the organizations on a heat matrix of risk and severity, with mitigation plans proposed accordingly.

#### 4.3.1. RRA

We used generalized linear models such as LR (Son et al., 2020) in the RRA module to test the hypotheses. Based on the chi-squared test, the goodness of fit of the model was revealed to be significant ($p < 0.001$) with a small deviance of 66.68. Table 8 reports the parameters of the M1 (LR) model that were significant at the 1% level.

Substituting the values from Table 8 into Equation (1), Eq. (3) is determined, as follows:

**Table 6**
Pairwise correlations among variables.

| | CI | size | DI | NS | EVSS | CSR | Type of Attack |
|---|---|---|---|---|---|---|---|
| CI | 1 | | | | | | |
| size | -0.042 | 1 | | | | | |
| DI | -0.121** | -0.074* | 1 | | | | |
| NS | -0.096** | -0.048 | 0.070* | 1 | | | |
| EVS | 0.009 | -0.055 | -0.049 | 0.048 | 1 | | |
| CSR | 0.000 | 0.215** | 0.034 | 0.004 | -0.070* | 1 | |
| Type of Attack | 0.170** | 0.204** | 0.143** | -0.141** | 0.052 | -0.024 | 1 |

* $p < 0.05$ (2-tailed)
* * $p < 0.01$ (2-tailed)

**Table 7**
Methodology for Ransomware Risk Assessment.

| Year | Authors | Features | | | | | | Methods | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Static | | Dynamic | | | | Rule | Machine-Learning-Based | | | | |
| | | *FI* | *op* | *RK* | *FP* | *PL* | *DLL* | Based | *SVM* | *RF* | *DT* | *NB* | *LR* |
| 2020 | Zuhair et al. | Y | | Y | Y | Y | Y | | | | Y | Y | |
| 2020 | Ramesh & Menen | Y | | Y | Y | Y | | Y | | | | | |
| 2019 | Zhang et al. | | Y | | | | | | | Y | Y | Y | |
| 2018 | Baldwin & Dehghantanha | | Y | | | | | | Y | | | | |
| 2018 | Cohen & Nissim | | | Y | Y | | Y | | | Y | | Y | Y |

FI: File Information; op: opcodes; RK: Registry Key; FP: File Process; PL: Pay-load; DLL: Dynamic Link Libraries; SVM: Support Vector Machine; RF: Random Forest; DT: Decision Tree; NB: Naïve Bayes; LR: Logistic Regression

**Table 8**
parameters obtained from M1 (LR) model.

| Variable | B | P value | Exp (B) | Hypothesis | Acceptance |
|---|---|---|---|---|---|
| Constant | -6.762 * | 0.001 | 0.001 | | |
| Size | 1.915 * | 0.001 | 6.786 | H1a | Supported |
| CI | 1.654 * | 0.001 | 5.229 | H1b | Supported |
| DI | 2.608 * | 0.001 | 13.573 | H2a | Supported |
| NS | -3.170 * | 0.001 | 0.042 | H2b | Supported |
| EVSS | 1.006 * | 0.098 | 2.734 | H3 | Supported |
| CSR | -0.866 * | 0.100 | 0.421 | H4 | Supported |

* indicates $p < 0.1$

$$\ln\left(\frac{P(C=R)}{P(C=NR)}\right) = -6.762 + 1.915(Size) + 1.654(CI) + 2.608(DI) - 3.170(NS) + 1.006(EVSS) - 0.866(\mathrm{CSR})\ldots \quad (3)$$

Table 8 and Eq. (3) indicate that larger organizations are 6.786 times more likely to face R attacks than NR attacks ($p = 0.001$), thereby supporting hypothesis H1a. Moreover, if organizations belong to a critical industry, their chances of facing ransomware attacks increase by 5.229 times compared to NR attacks ($p = 0.001$). This finding supports hypothesis H1b. Similarly, for each unit increase in digital intensity, the odds of R attacks are 13.573 times greater than those of NR attacks ($p = 0.001$). This result aligns with hypothesis H2a. However, if the network is segmented, the probability of occurrence of R attacks decreases to 0.042 times that of NR attacks ($p = 0.001$), thereby supporting hypotheses H2b. Table 8 also indicates that for each unit increase in vulnerabilities in the organizational environment, the odds of ransomware attacks increase by 2.734 times compared to other cyberattacks ($p = 0.098$). This finding supports hypothesis H3. In contrast, if information security governance is properly implemented in an organization, for an increase in every cybersecurity role, the probability of ransomware attacks decreases to 0.421 times that of non-ransomware attacks ($p = 0.100$), thereby supporting hypothesis H4.

Next, in the RRA module, we used the M1, M2, and M3 models to classify attacks as R or NR. The performances of the three models were measured and compared on the test dataset using the accuracy, precision, recall, and F1-score, as shown in Table 9.

It is evident from Table 9 that M1 was better than M2 and M3 because its accuracy, precision, recall, and F1-score were better than those of the other two models. Hence, this study further elaborates on the results of M1 (the LR model). Figs. 3(a) and 3(b) show that M1 could correctly classify or predict 27 out of 29 R and 293 out of 314 NR data points of the test dataset.

The likelihood of ransomware attacks, compared with the M1 model tended to follow a Weibull distribution (mean = 0.12, standard deviation = 1.12, scale parameter = 0.05, and shape parameter = 0.89). This means that large cyberattacks are infrequent in nature, and the frequency tends to decrease as patches are released for known vulnerabilities in IT systems. This finding is consistent with hypothesis H5a.

#### 4.3.2. RRQ

In the previous RRA step, M1 (LR) was considered to be better than M2 (NB) and M3 (DT). Hence, the M1 model of RRA was selected for further evaluation. The risk ($q_i$) obtained using LR was provided as input to the RRQ to compute the $EL_i$. The resultant severity or $EL_i$ followed a gamma distribution (mean = 1.9, standard deviation = 668.7, scale parameter = 1271.8, and shape parameter = 922.21). Large losses due to cyberattacks are few in number, whereas there are many smaller losses. This finding is consistent with hypothesis H5b.

#### 4.3.3. RRM

Based on $q$ and EL obtained from the RRA and RRQ, each data point of the test set was plotted on a $2 \times 2$ risk–severity heat matrix, as shown in Fig. 4. Each data point represents the risk exposure of an organization due to a ransomware attack. Most organizations that faced R attacks were in quadrant Q1 (high, high), with a few in Q4 (high, low). In contrast, more than 90% of the organizations that faced NR attacks were present in Q3 (low, low), with a few in Q2.

This study provides insight into the investments made by organizations in various quadrants of the PDDRRR ransomware mitigation strategies. Fig. 5(a) depicts the level of investment in the six phases of the ransomware risk mitigation strategies based on the quadrant of the risk–severity matrix in which the organization is positioned.

Fig. 5(a) shows that the organizations in Q1 (high, high) attempted to enhance their self-protection by investing in technological interventions, as indicated by the NIST Cybersecurity Framework (Harrison et al., 2022; NIST, 2022; Ramesh & Menen, 2020). They made higher investments (H-H-H-H-H-H) in the PDDRRR mitigation strategies, thereby moving from Q1 (high, high) to Q2 (high, low) and reducing the risk by 45.24% and severity by 50%, as shown in Fig. 5(b). This result supports hypothesis 6(a).

Fig. 5(a) shows that organizations in Q2 (high, low) made less technological investment in the preparation and deterring phases compared to other stages (L-L-H-H-H-H) of mitigation strategies (PDDRRR). They invested more in recovering the infected systems from the backup data, as suggested by the NIST Cybersecurity Framework

**Table 9**
Performance metrics of M1 (LR), M2 (NB), and, M3 (DT) classifiers.

| Model | Algorithms | Accuracy (p) | Misclassification rate (q=1-p) | Precision | Recall | F1 score |
|---|---|---|---|---|---|---|
| M1 | LR | 0.93 | 0.07 | 0.97 | 0.89 | 0.93 |
| M2 | NB | 0.90 | 0.10 | 0.66 | 0.81 | 0.66 |
| M3 | DT | 0.92 | 0.08 | 0.66 | 0.45 | 0.66 |

LR: Logistic Regression; NB: Naïve Bayes; DT: Decision Tree

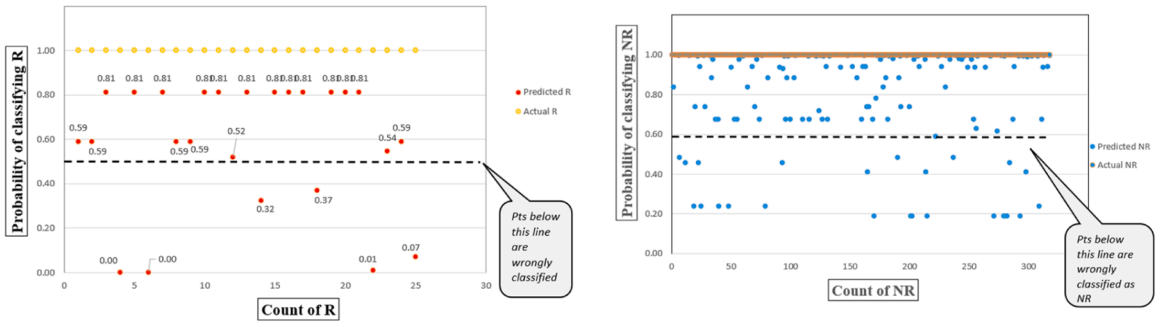



**Fig. 3.** a. LR results on the test dataset (R). b LR results on the test dataset (NR).

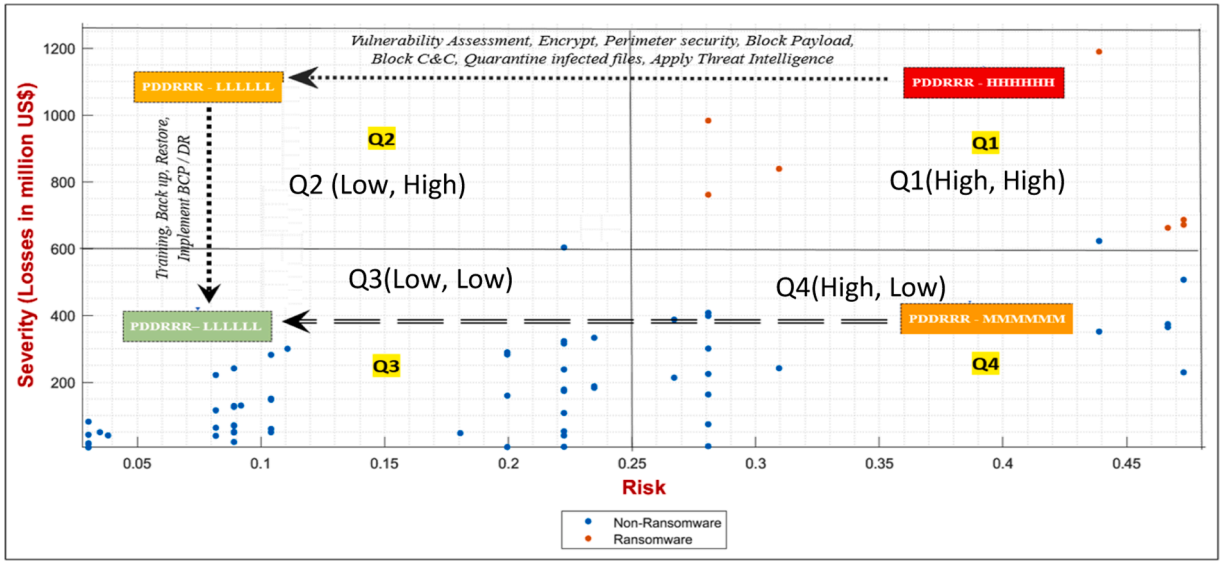
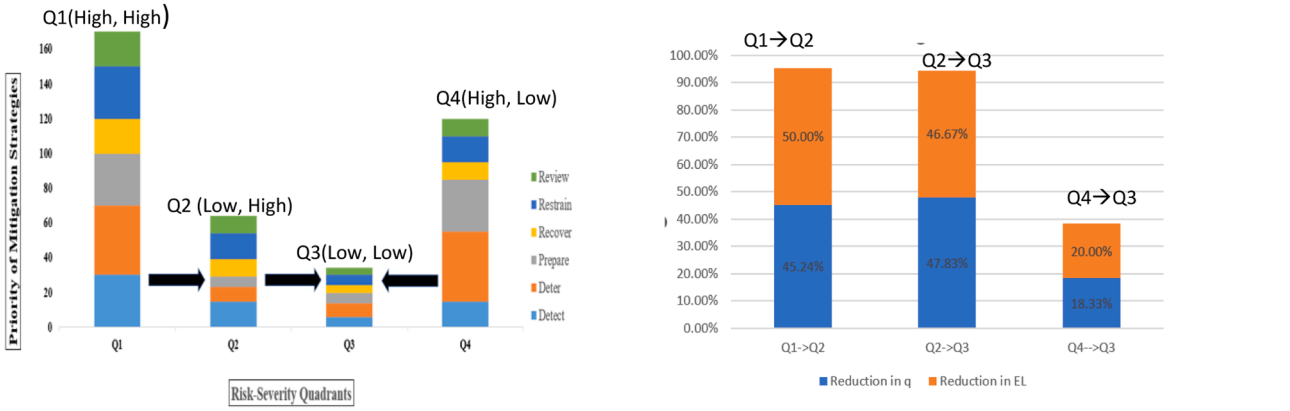



**Fig. 4.** Ransomware risk mitigation strategy for organization's based on their location on the heat matrix.




(a). Priorities of Mitigation Strategies (b). Reduction of risk and severity across quadrants

**Fig. 5.** (a). Priorities of Mitigation Strategies. (b). Reduction of risk and severity across quadrants.

(Harrison et al., 2022; NIST, 2022; Ramesh & Menen, 2020), thereby reducing the severity and consequently moving from Q2 (high, low) to Q3 (low, low) and reducing the risk by 47.83% and severity by 46.67%, as shown in Fig. 5(b). This finding supports Hypothesis 6b.

Fig. 5(a) indicates that the organizations in Q3 (low, low) maintained low overall technological investments (L-L-L-L-L-L) in all phases of the PDDRRR mitigation strategies. Once the organization reaches Q3 (low, low), it becomes eligible to transfer risk by investing in cyber-risk insurance (Muhly et al., 2022). This mitigation strategy is in accordance with previous studies (Straub & Welke, 1998; Mukhopadhyay et al., 2013). Once they can reduce their probability of attack and further reduce the severity of the attack, they can lower their cybersecurity investments, which is in accordance with COR theory. This result supports hypothesis 6c.

Finally, Fig. 5(a) shows that the organizations in Q4 (high, low) made high technological investments in the prepare and deter phases

(NIST, 2022) and moderate investments (H-H-M-M-M-M) in other phases of PDDRRR, thereby moving from Q4 (high, low) to Q3 (low, low) and reducing their risk by 18.33% and severity by 20%, as shown in Fig. 5(b). This result supports hypothesis 6d.

## 5. Qualitative study

### 5.1. Methodology

We interviewed participants from firms that had experienced a cyberattack, firms and consultants that provided these organizations with technological solutions, and cyber-risk insurers. For firms that had experienced cyberattacks, we interviewed people from multiple levels in the organization's cybersecurity, such as chief executive officers, chief risk managers, chief technology officers, CISOs, IT teams, cybersecurity consultants, and security architects. Next, we interviewed third-party vendors, such as managed security service providers, consultants, and perimeter security providers of EDR, XDR, SIEM, and SOAR. We also interviewed cyber insurance managers and underwriters. A total of 80 professionals, including practitioners and researchers, participated in the semi-structured interviews. Thereafter, we conducted data triangulation (Sarker et al., 2012) across participants belonging to firms that faced cyberattacks, consultants who provided them with technological solutions, and cyber-risk insurers.

We interviewed participants from firms that faced cyberattacks and consultants that provided these firms with technological solutions to establish the following dependencies: large firms in the critical sector with multiple channels of online distribution are prone to ransomware attacks, unless effective network segmentation is in place; the ransomware spreads easily across the firm; the severity of vulnerabilities in software, hardware, and networks are explored by hackers to compromise systems; and effective security governance practices and control can help to reduce ransomware attacks on the firm. Next, we interviewed cyber insurers to understand the frequency with which cyberattacks occur on a firm and their claim payout distributions. In addition, we attempted to understand how to mitigate risk by determining the proportion of accept, reduce, or transfer.

### 5.2. Results

#### 5.2.1. RRA

In this study, we use predictive analytics techniques to carry out a firm's ransomware risk assessment.

*5.2.1.1. Organizational structure.* The respondents highlighted that larger organizations, although better equipped with security technologies, can still be attacked by advanced persistent threat (APT) tools such as ransomware, which will cause serious business implications. Such attacks tend to bring the supply chain of the firm to a standstill. Chief Information Security Officer (CISO) of a firm noted that.

> "Large organizations like ours are facing a lot ransomware attacks lately. Unless you pay the ransom…which is a lot a money……in bitcoins ……. your daily operations come to a standstill. You lose a lot of business !!"

Representatives of a noted that Anti-virus company stated.

> "In the last few quarters, we have sold many end-point security (EPS) software to large organizations…. Our EPS has capabilities to alert and protect against ransomware"

If the healthcare, finance, or public administration delivery systems belonging to the critical sector are compromised by a hacker, the upstream and downstream of the value chain can be crippled. A manager of a firm in a critical sector highlighted that.

> "We could not access of our customer data, we could not fulfil orders, and shopfloor was idle and we were at loss."

A manager of a downstream firm along the value chain of the critical sector added:

> "We almost ran out of stock…. there was no replenishment coming in…. customer queues to the call centre and the store were piling up… it was really bad day. There was chaos all around"

*5.2.1.2. Technological factors.* Respondents noted that digital intensity of a firm increases its market footprint, and therefore, revenue. However, it also carries the inherent risk of being compromised by hackers, which can adversely effect their reputation and lead to customer churn. A manager of a firm in a critical sector said:

> **"**We have substantial revenues coming from the online channel. Our IT team tell me that the security operations Centre (SOC) is flooded with attempts by hackers to break in everyday"

The IT manager added.

> "I have to keep increasing my cost to project to ensure that the online operations are up, running and secure 24 × 7."

Cybersecurity domain experts believe that network segmentation within an organization helps to minimize the impact of ransomware attacks. A senior Security Architect noted.

> "Shrink the target and the impact zone through the principles of networking such as micro segmentation to combat ransomware. Network segmentation limits lateral movement, minimizing damage and reducing the risk of widespread compromise."

*5.2.1.3. Vulnerability assessment.* We found that security experts used an open framework or a universal language to understand the characteristics and severity of software, hardware, or network vulnerabilities in any organization. Chief Information Security Officer (CISO) of a firm noted that.

> "Constantly out IT team is on the lookout to prioritise out Cybersecurity efforts against ransomware attacks. How easy it is for attackers to exploit vulnerability in our system? What level of access is required to carry out a breach? Is easy or quite difficult to execute an attack? Finally assess the impact of the attack based what it comprises in the Confidentiality-Identity-Availability (CIA) triad"

*5.2.1.4. Information security governance.* Information security governance is the cornerstone of the cybersecurity posture of a firm. A well-defined governance structure ensures a coordinated incident response approach and enhances resilience against cyber threats. A strong framework promotes the rollout of effective controls, secure practices, and alignment with organizational objectives. Chief Information Security Officer of a firm noted that:

> "Success doesn't happen my chance. It's all about doing things well, doing things reliably by implementing the security controls. This will give your firm the expected outcomes".

Chief Risk Manager of a cyber risk insurance firm noted that.

> "we study the governance of a company …….who is in charge what sort of budget do

you have in place do you have a dedicated governance… who's managing the decision at the end of the day".

*5.2.1.5. Likelihood of a ransomware attack.* We observed that cyber-insurance providers examine the distribution of cyberattacks before determining their premiums. In this context, the Weibull distribution is

optimal. A cyber security team member noted that:

"There are a huge number of cyber attacks that last for a shorter period of time… however those that last for longer are usually low in count".

A cyber insurance underwriter stated that:

"we consider the distribution of cyber attacks while we decide for the premium payouts… we generally notice that there are multiple cyber attacks which are of shorter duration… accordingly our premium charges vary as per how the cyberattacks are distributed across the time"

#### 5.2.2. RRQ

The losses arising from ransomware attacks follow a long-tail distribution; that is, a gamma distribution. The CTO noted that:

"Our main focus is on the cyber-attacks that are few in count but incur huge damages… Wannacry as you know was a monster in this sense"

A cyber insurance underwriter stated that:

"Long tail distributions generally help us to understand cyber insurance claims… this is mainly because the expected losses due to cyber incidents are skewed in nature. "

#### 5.2.3. RRM

We created a heat-matrix (risk–severity) to understand the probability of a firm being attacked versus the impact of the ransomware-attack. Based on the location of the heat matrix, we propose a risk mitigation trajectory to be followed by the CISO of a firm by investing in security technology for PDDRRR. Cyber risk consultant stated that:

"heat matrix represents the organizational risk in a visually aiding format. Heat matrix tells you whether in in the high-high box or the low-low box or any other box. You can then plan for accept, reduce and transfer risk accordingly"

Another Cyber risk consultant stated that.

" To mitigate ransomware risk, we help the clients to understand what processes or assets inside their organization need protection. what safeguards or countermeasures they already have and what they need to get additionally… how to detect the security incidents quickly… what activities can help restrain the spread of ransomware… and last but not the least how to recover digital systems"

If a firm experiences a high likelihood of attack and a high impact of a ransomware attack, the CISO should attempt to reduce the cyber risk by investing in cybersecurity technology. CISO of a firm stated that.

"we have invested a lot of money in IT infrastructure protection, perimeter security, application security, identity access management, data security and backup to be resilient against ransomware attacks"

Chief Risk Manager of a cyber risk insurance firm noted that.

**"**we will generally recommend that CISO to implement proper controls like multi factor authentication, patch management, end point detection, cybers security awareness, cyber incidence response planning and testing, and digital supply chain management, this helps I risk reduction"

If a firm experiences a low likelihood of attack, but a high impact from a ransomware attack, the CISO should attempt to self-insure against cyber risk by investing in cybersecurity measures that reduce the severity of ransomware attacks. CISO of a firm stated that.

"cybersecurity essentially is an insurance… So any measure that one takes to improve the cybersecurity of their business is self-insurance in this space… The flip side to that is very few events will finish your business since it's not really a super huge focus, especially if it's not one that they've encountered before… So you literally are going to the casino if you don't have anything in place."

CTO of a firm stated that.

"if you can afford to take the bumps you know some unusual expense coming along doesn't really hurt you that much why would you waste your money paying the insurance premiums… Invest in your BCP DR activities so as to minimize your cyber attack losses…"

If a firm experiences a low likelihood of attack and low impact from a cyberattack, it can opt for cyber-risk insurance to transfer the residual cyber risk and protect itself from future losses against a ransomware attack. Chief Risk Manager of a cyber risk insurance stated that:

" buying cyber risk insurance about risk transfer. I's all about technology plus cyber risk insurance to offload that risk."

Another Cyber risk underwriter said.

"We complement all of your plans and risk management and reinforce your resilience.

it's not there to replace security it's there as an additional tool".
CEO of a firm stated that.

"Board of governors in our firm deals with the risk including operational risks. They also suggest we take cyber risk insurance against downtime, and loss customer data"

If a firm experiences a high likelihood of cyberattack but with a low impact from the attack, it can opt for self-insurance; that is, investments in cyber technological interventions such as firewalls, antivirus, and IDPs/IPSs, to reduce the probability of ransomware attacks. CTO states that:

"Anything you invest into to defend your boundaries from bad actors. or to reduce the chances of your organization getting hit by these cyber threats. is a self- insurance. when I know that my likelihood of getting attacked is high. may be because I operate in a critical sector the cyber attackers have their eyes on…then why would I not keep my money aside in strengthening my peripheries…"

Cyber security team expert quoted:

"When my company started investing in pre-attack mitigation strategies. I see a huge drop in the cyber security events."

## 6. Discussion

This study has used a mixed-method explanatory approach (Ballerini et al., 2023; Dwivedi et al., 2021; Kar & Dwivedi, 2020; Maier et al., 2023; Mikalef et al., 2019; Wunderlich et al., 2019) to examine the research questions. First, the quantitative R2M2 was developed. The R2M2 model consists of three modules. The RRA module lists the possible causes of a ransomware attack. We tested our hypotheses using the generalized linear models. We found that larger organizations are more susceptible to such attacks, which is consistent with previous studies that highlighted the attractiveness of such organizations to ransomware attackers because of their ability to pay larger ransoms and their possession of critical data (Angst et al., 2017; Brewer, 2016; Mansfield-Devine, 2016). However, regardless of their size, organizations should invest in countermeasures (Yuryna Connolly et al., 2020). The results also indicate that organizations belonging to critical industries are prone to ransomware attacks, which aligns with previous studies that highlighted the critical nature of these daily operations as an enticing target for attackers (Javed Butt et al., 2019). Previous studies also showed that firms in the critical sector tend to have low risk tolerance to ransomware attacks (Samonas et al., 2020; Tsen et al.,

2022) and tend to address known vulnerabilities (CERT-In, 2023). In addition, the findings demonstrate that organizations with high digital intensity have an increased risk of ransomware attacks, as also indicated by previous studies (Kim & Kwon, 2019; McLeod & Dolezel, 2018; Smith et al., 2021). Furthermore, the results indicate that network segmentation in firms decreases the likelihood of ransomware attacks because it hinders the lateral movement of ransomware traffic, thereby maintaining critical files or servers separate from internet entry points. This aligns with the findings of previous studies (Conti et al., 2018; Shu et al., 2017).

The results demonstrate that organizations with higher vulnerability tend to have a higher probability of facing ransomware attacks. This aligns with previous studies that emphasized the role of employees (Wong et al., 2022) as a weak link in cybersecurity, despite significant investments in IT security (FIRST, 2019; Zhuang et al., 2020). Attackers exploit social engineering to target such employees, leading to breaches in CIA (O'Kane et al., 2018; Oz et al., 2022). Fewer restrictive privileges required to run an application also contribute to increased vulnerability (Peters, 2017).

Finally, the findings confirm that effective information security governance reduces the likelihood of ransomware attacks. The presence of CSR within organizations ensures the proper implementation of IT controls, thereby enhancing cybersecurity (Fazlida & Said, 2015; Weixun Li et al., 2023).

As in previous studies (Bardhan et al., 2015; Biswas et al., 2022; Lin et al., 2017; Mukhopadhyay et al., 2019), the probability of ransomware attacks was computed using predictive analytics such as LR. The probability of ransomware attacks follows a Weibull distribution (Hossack et al., 1983), whereas the expected losses exhibit a gamma distribution (Dutta & Perry, 2006; Mukhopadhyay et al., 2019).

Our qualitative study also validated the findings of the quantitative study (Ballerini et al., 2023; Dwivedi et al., 2021; Kar & Dwivedi, 2020; Maier et al., 2023; Mikalef et al., 2019; Wunderlich et al., 2019). We could reinforce these relationships by conducting interviews with respondents from firms that had experienced a cyberattack, firms and consultants that provided them with technological solutions, and cyber-risk insurers. It was confirmed that large firms in the critical sector with multiple channels of online distribution are prone to ransomware attacks unless they have effective network segmentation, if they have unpatched severe vulnerabilities in software, hardware, and networks, and if they do not implement effective security governance practices and control. We also noted that cyber-insurers tend to focus on learning the frequency of cyberattacks and their impact. Finally, the CISO determines the proportion of risk to accept, reduce or transfer.

### 6.1. Theoretical contributions

The quantitative R2M2 contributes to the literature by holistically assessing, quantifying, and mitigating ransomware attacks by considering the concepts of PMT (Li et al., 2019), COR theory, RCT, trade-off theory, and the NIST Cybersecurity Framework. Previous studies mainly focused on variables related to ransomware binaries (i.e., static or dynamic features). However, the proposed RRA module considers the process view of a ransomware attack as guided by the CKC. The attacker performs reconnaissance of the IT environment of an organization and exploits its vulnerabilities. Hence, this study considered the severity of the vulnerabilities to assess the ransomware risk to an organization. Moreover, it considered the implementation of information security governance and other cybersecurity measures deployed by an organization, such as the encryption of data and segmentation of networks, to neutralize the CKC. We used predictive analysis techniques such as NB, DT, and LR to determine the likelihood of a ransomware versus non-ransomware attack. The RRQ module contributes to the quantification of the ransomware risk from a financial perspective and indicates that the likelihood of a ransomware attack follows a Weibull distribution, whereas its severity follows a gamma distribution. Finally, the RRM module helps the CISO to visualize the risk and severity of the attack to which the organization is exposed on a heat matrix. Finally, the proposed mitigation techniques for the CISO are based on academic solutions (Straub & Welke, 1998) and the NIST Cybersecurity Framework, which is commonly used industry practice (NIST, 2014b, 2018). The proposed best practices, such as vulnerability assessment, block payload delivery, and block C&C communication, are primarily for pre- and post-ransomware attacks. The model uses a cost-benefit analysis (Gordon et al., 2003a) in the background based on the risk and severity as per the heat matrix before proposing the technological intervention to reduce the risk, followed by self-insurance and cyber-risk insurance. Based on the risk severity portfolio, the technological investments into the PDDRRR mitigation strategies (NIST, 2022) can be prioritize. For instance, an organization deters attackers by ensuring that the information is encrypted such that even if they have access to it, they are unable to decipher it. Likewise, regularly backing up an organization's data will help restore it in the event of information theft. Finally, the model suggests how organizations can increase their eligibility to cover the residual risks of cyber insurance. Our qualitative study also validated the findings of the quantitative study (Ballerini et al., 2023; Dwivedi et al., 2021; Kar & Dwivedi, 2020; Maier et al., 2023; Mikalef et al., 2019; Wunderlich et al., 2019). We could reinforce these relationships by conducting interviews with respondents from firms that had experienced a cyberattack, firms, and consultants that provided them with technological solutions, and cyber-risk insurers.

### 6.2. Implications for practice

Our study can help the CISO to assess the risk and severity of ransomware attacks. First, we recommend that the CISO of a large organization operating in the critical sector (such as healthcare, power and energy, infrastructure, and finance) has multiple online channels that are frequently prone to reconnaissance studies by hackers. To minimize such attacks, the CISO should invest in perimeter security elements such as firewalls, antivirus, and IDSs, and encrypt their data. This will help to prevent a ransomware attack vector from attacking the IT systems of these organizations. We would also advise the CISO to carry out regular training programs to sensitize and create awareness among employees against clicking on phishing emails, as this is the most common mechanism for delivering the payload to the IT system of an organization. Following this cyber-hygiene strategy will help the CISO to impose a strict cyber-posture against ransomware attacks. Second, we recommend that the CISO implements a network segmentation strategy to reduce the probability of the ransomware vector not traveling across the organizational network. The main objective of the CISO is to ensure that the ransomware cannot install any payload on the IT assets. Third, the CISO should carry out a vulnerability assessment to understand the points of weakness in software, hardware, and networks. The CISO should ensure that the vulnerabilities are patched regularly so that the hacker does not access execute an attack, which could lead to a compromise of the CIA triad. Fourth, the CISO should ensure that IT governance practices are effectively rolled out, so that the hacker is deterred from breaching the IT assets, communicating to the remote C&C center, encrypting it, and in some cases, exfiltrating the data. Fifth, our study can help the CISO to determine the likelihood of ransomware attacks. On this basis, the CISO can plan investments in cybersecurity elements to deter ransomware attacks. Sixth, this study can provide the CISO with an estimate of the expected loss if a ransomware attack occurs. Seventh, the study can help the chief technology officer to visualize the cyber-risk status of the firm on a heat matrix (likelihood of attack $\times$ impact of attack). The model will help the CISO to decide on technological investments (NIST, 2022) for PDDRRR mitigation strategies and to assign priorities (high/medium/low). These mitigation strategies are in accordance with well-established industry frameworks, such as the NIST Cybersecurity Framework, for warding off cyberattacks. Eighth, if an organization faces a high probability and high severity of a

ransomware attack, the model suggests that the CISO prioritizes investments in cybersecurity technologies for PDDRRR. For instance, the CISO should regularly monitor the digital assets and processes of the firm by performing vulnerability assessments and penetration testing. This is because our model informs the CISO that the severity of vulnerabilities in the IT environment is directly proportional to the likelihood of an organization being attacked by ransomware. These technological investments will help the CISO to reduce the probability and severity of ransomware attacks. Ninth, if the organization faces a high probability and low severity of a ransomware attack, the model proposes that the CISO should focus on reducing the probability of a ransomware attack through self-insurance. This would include allocating sufficient budgets tosecurity technologies. For instance, data can be encrypted and and backed up, network segmentation can be implemented to contain ransomware attacks by blocking payload delivery, and BCP/DR can be implemented. Tenth, if the organization faces a low probability and high severity of a ransomware attack, the CISO can invest in technologies that can minimize the losses due to the ransomware attack. Finally, if the organization faces a low risk and low severity of ransomware attacks, the CISO can invest in cyber insurance to transfer the residual risk and protect the organization from future ransomware attacks. Using this model, the CISO can visualize the increasing strength of ransomware techniques with burgeoning information technology capabilities, such as unbreakable encryption (AES 256-bit encryption), anonymous payments (cryptocurrency), platform agnostic ransomware (RaaS), and target-specific attacks (TickBots). This will motivate the CISO to enhance cybersecurity investments as the technological capabilities of the firm increase and improve the cybersecurity posture of the firm. This can help to protect firms from facing downtime and customer churn and, consequently, losing their reputation.

### 6.3. Limitations and future research

A limitation of this study is that limited organizational features were considered owing to the scarcity of data. This is mainly because firms facing ransomware attacks are reluctant to share the profile or attack data of their organizations. Future studies can also examine other parameters to determine the importance of ransomware risk mitigation strategies. One such parameter could be the strategic goals of firms. The cybersecurity mitigation methods can be prioritized based on the strategic IT plan of an organization.

## 7. Conclusion

This study has used a mixed-method explanatory approach to propose a the R2M2 model that holistically assesses, quantifies, and mitigates ransomware. We assessed ransomware attack risk using the organizational structure, network characteristics, and environmental vulnerability score as inputs. Next, the expected loss due to a ransomware attack on a firm in critical industry was estimated. We also positioned each firm in a heat matrix (probability of attack $\times$ impact). This model informs the CISO of the probability of a ransomware attack on the firm and the corresponding estimated loss due to the attack. The model also provides a mitigation strategy for the CISO of a firm that is located in the (high, high) quadrant of the heat matrix to resort to self-protection by investing in cybersecurity technologies, regular monitoring of digital assets and processes, safeguarding the perimeters of the organization, effectively segmenting the network, backing up and encrypting the data, training the employees, and creating awareness among employees regarding ransomware attack risk, as well as implementing control and information security governance strategies. If the firm lies in the (high, low) and (low, high) quadrants, the CISO should opt for self-insurance; that is, invest in cyber technology tools to reduce the probability of a ransomware attack and then create a contingency fund to make good the loss arising from a ransomware attack on the firm. If the firm lies in the (low, low) quadrant of the heat matrix, the CISO can transfer the cyber risk to a cyber-risk insurer upon payment of a premium. Finally, we validated the above findings through a qualitative study by interviewing participants from firms affected by ransomware, managed security service providers, security consultants, and cyber-risk insurers.

## Declaration of Competing Interest

With the submission, the authors confirm no conflict of interest. We also confirm that the manuscript is not published or under consideration elsewhere.

## Acknowledgement

The study is funded by Cyber Security Division, Ministry of Electronics and Information Technology, Government of India [AAA.22/1/2022-CSRD-MeitY].

## References

Abbasi, A., Albrecht, C., Vance, A., Hansen, J., Albrecht, C., Vance, A., & Hansen, J. (2012). MetaFraud: A meta-learning framework for detecting financial fraud. *MIS Quarterly: Management Information Systems, 36*(4), 1293–1327.

Agresti, A. (2002). *Categorical Data Analysis*. Wiley. https://doi.org/10.1002/0471249688

Akbanov, M., Vassilakis, V. G., & Logothetis, M. D. (2019). WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. *Journal of Telecommunications and Information Technology, 1*, 113–124. https://doi.org/10.26636/jtit.2019.130218

Almashhadani, A. O., Kaiiali, M., Sezer, S., & O'Kane, P. (2019). A multi-classifier network-based crypto ransomware detection system: A case study of locky ransomware. *IEEE Access, 7*, 47053–47067. https://doi.org/10.1109/ACCESS.2019.2907485

Al-Rimy, B. A. S., Maarof, M. A., Prasetyo, Y. A., Shaid, S. Z. M., & Ariffin, A. F. M. (2018). Zero-day aware decision fusion-based model for crypto-ransomware early detection. *International Journal of Integrated Engineering, 10*(6), 82–88. https://doi.org/10.30880/ijie.2018.10.06.011

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly, 41*(3), 893–916. https://doi.org/10.25300/MISQ/2017/41.3.10

Aoyama, T., Naruoka, H., Koshijima, I., Machii, W., & Seki, K. (2015). Studying resilient cyber incident management from large-scale cyber security training. *10th Asian Control Conference (ASCC)*, 1–4. https://doi.org/10.1109/ASCC.2015.7244713

Arad, S., Hanson, M. A., & Schneider, R. J. (1997). A framework for the study of relationships between organizational characteristics and organizational innovation. *The Journal of Creative Behavior, 31*(1), 42–58. https://doi.org/10.1002/j.2162-6057.1997.tb00780.x

Arghandeh, R., von Meier, A., Mehrmanesh, L., & Mili, L. (2016). On the definition of cyber-physical resilience in power systems. *Renewable and Sustainable Energy Reviews, 58*, 1060–1069. https://doi.org/10.1016/j.rser.2015.12.193

Baek, S., Jung, Y., Mohaisen, D., Lee, S., & Nyang, D. (2021). SSD-assisted ransomware detection and data recovery techniques. *IEEE Transactions on Computers, 70*(10), 1762–1776. https://doi.org/10.1109/TC.2020.3011214

Baldwin, J., & Dehghantanha, A. (2018). Leveraging support vector machine for opcode density based detection of crypto-ransomware. In A. Dehghantanha, M. Conti, & T. Dargahi (Eds.), *Cyber Threat Intelligence*. Springer International Publishing. https://doi.org/10.1007/978-3-319-73951-9_6.

Ballerini, J., Herhausen, D., & Ferraris, A. (2023). How commitment and platform adoption drive the e-commerce performance of SMEs: A mixed-method inquiry into e-commerce affordances. *International Journal of Information Management, 72*, Article 102649. https://doi.org/10.1016/j.ijinfomgt.2023.102649

Bardhan, I., Oh, J. H., Zheng, Z., & Kirksey, K. (2015). Predictive analytics for readmission of patients with congestive heart failure. In *Information Systems Research, 26* pp. 19–39). https://doi.org/10.1287/isre.2014.0553

Baskerville, R. L., Straub, D. W., & Goodman, S. (2008). Strategic information security risk management. *Information Security Policy, Processes, and Practices*, 112–122.

Becker, G. (1990). *The Economic Approach to Human Behavior*. University of Chicago Press.

Ben-Assuli, O., & Padman, R. (2020). Trajectories of repeated readmissions of chronic disease patients: Risk stratification, profiling, and prediction. *MIS Quarterly: Management Information Systems, 44*(1), 201–226. https://doi.org/10.25300/MISQ/2020/15101

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. v (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly*, 471–482.

Biswas, B., Mukhopadhyay, A., Kumar, A., & Delen, D. (2023). A hybrid framework using explainable AI (XAI) in cyber-risk management for defence and recovery against phishing attacks. *Decision Support Systems*. , Article 114102. https://doi.org/10.1016/j.dss.2023.114102

Biswas, B., Mukhopadhyay, A., Bhattacharjee, S., Kumar, A., & Delen, D. (2022). A text-mining based cyber-risk assessment and mitigation framework for critical analysis of

online hacker forums. *Decision Support Systems, 152*, Article 113651. https://doi.org/10.1016/j.dss.2021.113651
Bodeau, D., Boyle, S., & Fabius-greene, J. (2010). *Cyber Security Governance A Component of MITRE ' s Cyber Prep Methodology* (Issue September).
Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5
Bowen, P., & Wilson, M. (2006). *Information Security Handbook: A Guide for Managers* (Issue October). ⟨http://csrc.nist.gov/publications/nistpubs/800–100/SP800–100-Mar07–2007.pdf⟩.
Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. *Network Security, 2016*(9), 5–9. https://doi.org/10.1016/S1353-4858(16)30086-1
Campbell, D. E., & Kelly, J. S. (1994). Trade-off theory. *The American Economic Review, 84* (2), 422–426. ⟨http://www.jstor.org/stable/2117871⟩.
Carias, J. F., Labaka, L., Sarriegi, J. M., & Hernantes, J. (2018). An Approach to the Modeling of Cyber Resilience Management. *2018 Global Internet of Things Summit (GIoTS)*, 1–6. https://doi.org/10.1109/GIOTS.2018.8534579
Carroll, D. A., & Stater, K. J. (2008). Revenue diversification in nonprofit organizations: Does it lead to financial stability? *Journal of Public Administration Research and Theory, 19*(4), 947–966. https://doi.org/10.1093/jopart/mun025
CERT-In. (2023). *Vulnerability Notes*. ⟨https://cert-in.org.in/⟩.
Chanias, S., Myers, M. D., & Hess, T. (2019). Digital transformation strategy making in pre-digital organizations: The case of a financial services provider. *The Journal of Strategic Information Systems, 28*(1), 17–33. https://doi.org/10.1016/j.jsis.2018.11.003
Chen, P.-H., Bodak, R., & Gandhi, N. S. (2021). Ransomware recovery and imaging operations: Lessons learned and planning considerations. *Journal of Digital Imaging, 34*(3), 731–740. https://doi.org/10.1007/s10278-021-00466-x
CISA. (2022). *Detection and Prevention*. CISA. ⟨https://www.cisa.gov/detection-and-prevention⟩.
COBIT. (2007). *Effective IT Governance at Your Fingertips*. ⟨https://www.isaca.org/resources/cobit⟩.
Cohen, A., & Nissim, N. (2018). Trusted detection of ransomware in a private cloud using machine learning methods leveraging meta-features from volatile memory. *Expert Syst Appl, 102*(C), 158–178. https://doi.org/10.1016/j.eswa.2018.02.039
Connolly, L. Y., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security, 87*, Article 101568.
Conti, M., Gangwal, A., & Ruj, S. (2018). On the economic significance of ransomware campaigns: A Bitcoin transactions perspective. *Computers & Security, 79*, 162–189. https://doi.org/10.1016/j.cose.2018.08.008
Dalton, D. R., Todor, W. D., Spendolini, M. J., Fielding, G. J., & Porter, L. W. (1980). Organization structure and performance: A critical review. *The Academy of Management Review, 5*(1), 49–64. https://doi.org/10.2307/257804
Dargahi, T., Dehghantanha, A., Bahrami, P. N., Conti, M., Bianchi, G., & Benedetto, L. (2019). A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. *Journal of Computer Virology and Hacking Techniques, 15*(4), 277–305. https://doi.org/10.1007/s11416-019-00338-7
Das, S., Mukhopadhyay, A., Saha, D., & Sadhukhan, S. (2019). A markov-based model for information security risk assessment in healthcare MANETs. *Information Systems Frontiers, 21*(5), 959–977. https://doi.org/10.1007/s10796-017-9809-4
DeLone, W. H. (1981). Firm size and the characteristics of computer use. *MIS Quarterly, 5* (4), 65–77. https://doi.org/10.2307/249328
Dutta, K., & Perry, J. (2006). *A tale of tails: an empirical analysis of loss distribution models for estimating operational risk capital*.
Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., … Williams, M. D. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management, 57*, Article 101994. https://doi.org/10.1016/j.ijinfomgt.2019.08.002
Ein-Dor, P., & Segev, E. (1978). Organizational context and the success of management information systems. *Management Science, 24*(10), 1064–1077. ⟨http://www.jstor.org/stable/2630560⟩.
Fazlida, M. R., & Said, J. (2015). Information security: Risk, governance and implementation setback. *Procedia Economics and Finance, 28*, 243–248. https://doi.org/10.1016/S2212-5671(15)01106-5
FIRST. (2019). *Common Vulnerability Scoring System version 3.1 Specification Document*. 1–24. ⟨https://www.first.org/cvss/⟩.
Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003a). Information security expenditures and real options: A wait-and-see approach. *Computer Security Journal, 19*(2), 1–7.
Gordon, L. A., Loeb, M. P., & Sohail, T. (2003b). A framework for using insurance for cyber-risk management. *Communications of the ACM, 46*(3), 81–85.
Han, J., Kamber, M., & Pei, J. (2012). Data Mining. In J. Han, M. Kamber, & J. Pei (Eds.), *Data Mining (Third Edition)* (Third Edit, pp. 393–442). Morgan Kaufmann. https://doi.org/https://doi.org/10.1016/B978–0-12–381479-1.00009–5.
Harrison, A. S., Sullivan, P., Kubli, A., Wilson, K. M., Taylor, A., DeGregorio, N., Riggs, J., Werner-Wasik, M., Dicker, A., & Vinogradskiy, Y. (2022). How to respond to a ransomware attack? One radiation oncology department's response to a cyber-attack on their record and verify system. *Practical Radiation Oncology, 12*(2), 170–174. https://doi.org/10.1016/j.prro.2021.09.011
Hobfoll, S. E., Shirom, A., & Golembiewski, R. (2000). Conservation of resources theory. *Handbook of Organizational Behavior*, 57–80.
Hossack, I., Pollard, J., & Zehnwirth, B. (1983). *Introductory Statistics with Applications in General Insurance, 1* pp. 1–282). *Cambridge*: Cambridge University Press.
IBM Security. (2022). *Definitive Guide to Ransom*ware 2022.
IBM. (2022). *What is Security Information and Event Management (SIEM)?* IBM. ⟨https://www.ibm.com/in-en/topics/siem⟩.
Jain, S., & Mukhopadhyay, A. (2023). Vulnerability-based Cyber-Risk Management: A Text-mining Approach. *AMCIS 2023 Proceedings*, 17. ⟨https://aisel.aisnet.org/amcis2023/sig_sec/sig_sec/17⟩.
Jain, S., Mukhopadhyay, A., & Jain, S. (2023). Can cyber risk of health care firms be insured? A multinomial logistic regression model. *Journal of Organizational Computing and Electronic Commerce, 33*(1-3), 41–69. https://doi.org/10.1080/10919392.2023.2244386
Javed Butt, U., Abbod, M., Lors, A., Jahankhani, H., Jamal, A., & Kumar, A. (2019). Ransomware Threat and its Impact on SCADA. 2019 *IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, 205–212. https://doi.org/10.1109/ICGS3.2019.8688327.
Kahane, Y., Neumann, S., & Tapiero, C. S. (1988). Computer backup pools, disaster recovery, and default risk. *Communications of the ACM, 31*(1), 78–83.
Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics, 139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019
Kar, A. K., & Dwivedi, Y. K. (2020). Theory building with big data-driven research – Moving away from the "What" towards the "Why". *International Journal of Information Management, 54*, Article 102205. https://doi.org/10.1016/j.ijinfomgt.2020.102205
Kim, S. H., & Kwon, J. (2019). How do EHRs and a meaningful use initiative affect breaches of patient information? *Information Systems Research, 30*(4), 1184–1202. https://doi.org/10.1287/isre.2019.0858
Kleindorfer, P. R., & Kunreuther, H. (1999). The complementary roles of mitigation and insurance in managing catastrophic risks. *Risk Analysis, 19*(4), 727–738.
Kunreuther, H. (1997). Managing Catastrophic Risks Through Insurance And Mitigation. *"Financial Risk Management for Natural Catastrophes " Gold Coast, Australia*, 1–31.
Kunreuther, H., & Heal, G. (2003). Interdependent Security. *Journal of Risk and Uncertainty, 26*(2), 231–249. https://doi.org/10.1023/A:1024119208153
Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017
Lin, A.Y., Chen, H., Brown, R.A., Li, S., Yang, H., & Lin, Y. (2017). *Healthcare Predictive Analytics for Risk Profiling In Chronic Care: A Bayesian Multitask Learning Approach. 41* (2), 473–496.
Liu, C.-W., Huang, P., & Lucas, H. C. (2020). Centralized IT decision making and cybersecurity breaches: Evidence from U.S. higher education institutions. *Journal of Management Information Systems, 37*(3), 758–787. https://doi.org/10.1080/07421222.2020.1790190
Lockheed Martin. (2011). *The Cyber Kill Chain*. ⟨https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html⟩.
Mikalef, P., Boura, M., Lekakos, G., & Krogstie, J. (2019). Big data analytics and firm performance: Findings from a mixed-method approach. *Journal of Business Research, 98*, 261–276.
Maier, C., Thatcher, J. B., Grover, V., & Dwivedi, Y. K. (2023). Cross-sectional research: A critical perspective, use cases, and recommendations for IS research. *International Journal of Information Management, 70*, Article 102625. https://doi.org/10.1016/j.ijinfomgt.2023.102625
Mansfield-Devine, S. (2016). Ransomware: taking businesses hostage. *Network Security, 2016*(10), 8–17. https://doi.org/10.1016/S1353-4858(16)30096-4
McCarthy, B. (2002). New economics of sociological criminology. *Annual Review of Sociology*, 417–442.
McCullagh, P., & Nelder, J. A. (1989). *Generalized linear models*. Springer US. https://doi.org/10.1007/978-1-4899-3242-6
McIntosh, T., Kayes, A. S. M., Chen, Y.-P. P., Ng, A., & Watters, P. (2022). Ransomware mitigation in the modern Era: A comprehensive review, research challenges, and future directions. *ACM Computing Surveys, 54*(9), 1–36. https://doi.org/10.1145/3479393
McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems, 108*, 57–68. https://doi.org/10.1016/j.dss.2018.02.007
Meijer, M., Smalley, M., Taylor, S., & Dunwoodie, C. (2013). ITIL® and BiSL®: sound guidance for business-IT alignment from a business perspective. *The Stationary Office AXELOS Whitepaper*, 1–8.
Meshkat, L., & Miller, R. L. (2022). Quantifying Cybersecurity Risk for NASA Missions. *2022 Annual Reliability and Maintainability Symposium (RAMS)*, 1–7. https://doi.org/10.1109/RAMS51457.2022.9893983
Mos, M.A., & Chowdhury, M.M. (2020). The Growing Influence of Ransomware. *IEEE International Conference on Electro Information Technology, 2020-July*, 643 – 647. https://doi.org/10.1109/EIT48999.2020.9208254.
Muckin, M., & Fitch, S. C. (2019). A threat-driven approach to cyber security. *Lockheed Martin Corporation*, 1–45.
Muhly, F., Işik, Ö., & Leo, P. (2022). *The Ransomware Dilemma*. MIT Sloan Management Review. ⟨https://sloanreview.mit.edu/article/the-ransomware-dilemma/⟩.
Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems, 56*(1), 11–26. https://doi.org/10.1016/j.dss.2013.04.004
Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2019). Cyber risk assessment and mitigation (CRAM) framework using logit and probit models for cyber insurance. *Information Systems Frontiers, 21*(5), 997–1018. https://doi.org/10.1007/s10796-017-9808-5

NIST. (2014a). *NIST SP 800–12: Chapter 15 - Physical and Environmental Security*. ⟨https://csrc.nist.rip/publications/nistpubs/800–12/800–12-html/chapter15.html⟩.
NIST. (2014b). *Framework for Improving Critical Infrastructure Cybersecurity*. ⟨https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf⟩.
NIST. (2018, April 16). *The Five Functions*. NIST. https://doi.org/10.6028/NIST.CSWP.04162018.
NIST. (2022). *Getting Started with Cybersecurity Risk Management: Ransomware* (Issue February).
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
Ochoa, R., Ticse, Di, Herrera, E., & Vargas, J. (2021). Ransomware scenario oriented financial quantification model for the financial sector. *Proceedings of the 2021 IEEE Sciences and Humanities International Research Conference, SHIRCON 2021*. https://doi.org/10.1109/SHIRCON53068.2021.9652252.
Ou, C. X., Zhang, X., Angelopoulos, S., Davison, R. M., & Janse, N. (2022). Security breaches and organization response strategy: Exploring consumers' threat and coping appraisals. *International Journal of Information Management, 65*, Article 102498. https://doi.org/10.1016/j.ijinfomgt.2022.102498
Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys*. https://doi.org/10.1145/3514229
Patel, S. C., Graham, J. H., & Ralston, P. A. S. (2008). Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements. *International Journal of Information Management, 28*(6), 483–491. https://doi.org/10.1016/j.ijinfomgt.2008.01.009
Peters, J. (2017). *How to Organize and Classify Different Aspects of Cyber Threat Intelligence*. SurfWatch Labs Inc. ⟨https://blog.surfwatchlabs.com/2017/10/02/how-a-mind-map-can-help-organizations-better-understand-threat-intelligence/⟩.
Ramesh, G., & Menen, A. (2020). Automated dynamic approach for detecting ransomware using finite-state machine. *Decision Support Systems, 138*(January), Article 113400. https://doi.org/10.1016/j.dss.2020.113400
Raymond, L. (1985). Organizational characteristics and MIS success in the context of small business. *MIS Quarterly, 9*(1), 37. https://doi.org/10.2307/249272
Rogers, R. W. (1975a). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803
Rogers, R. W. (1975b). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803
Samonas, S., Dhillon, G., & Almusharraf, A. (2020). Stakeholder perceptions of information security policy: Analyzing personal constructs. *International Journal of Information Management, 50*, 144–154. https://doi.org/10.1016/j.ijinfomgt.2019.04.011
Sarker, S., Sarker, S., Sahaym, A., & Bjørn-Andersen, N. (2012). Exploring value cocreation in relationships between an ERP vendor and its partners: A revelatory case study. *MIS Quarterly, 36*(1), 317–338. https://doi.org/10.2307/41410419
Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. *Information & Management, 59*(4), Article 103638. https://doi.org/10.1016/j.im.2022.103638
Sharma, K., & Mukhopadhyay, A. (2022). Sarima-based cyber-risk assessment and mitigation model for a smart city's traffic management systems (Scram). *Journal of Organizational Computing and Electronic Commerce, 32*(1), 1–20. https://doi.org/10.1080/10919392.2022.2054259
Sharma, K., & Mukhopadhyay, A. (2023). Cyber-risk Management Framework for Online Gaming Firms: an Artificial Neural Network Approach. *Inf Syst Front, 25*, 1757–1778. https://doi.org/10.1007/s10796-021-10232-7
Shu, X., Tian, K., Ciambrone, A., & Yao, D. (2017). Breaking the Target: An Analysis of Target Data Breach and Lessons Learned. *Cryptography and Security*. ⟨http://arxiv.org/abs/1701.04940⟩.
Smith, T., Tadesse, A. F., & Vincent, N. E. (2021). The impact of CIO characteristics on data breaches. *International Journal of Accounting Information Systems, 43*, Article 100532. https://doi.org/10.1016/j.accinf.2021.100532
Son, J., Brennan, P. F., & Zhou, S. (2020). A data analytics framework for smart asthma management based on remote health information systems with bluetoothenabled personal inhalers. *MIS Quarterly: Management Information Systems, 44*(1), 285–303. https://doi.org/10.25300/MISQ/2020/15092
Souppaya, M., & Scarfone, K. (2013). Guide to Malware Incident Prevention and Handling for Desktops and Laptops. In *NIST Special Publication* (Vol. 800). http://dx.doi.org/10.6028/NIST.SP.800–83r1%0A.
Statista. (2022). *Amount of monetary damage caused by reported cyber crime to the IC3 from 2001 to 2021 (in million U.S. dollars)*. Statista 2022. ⟨https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/⟩.
Stolk, V. (2022). *You Win Some You Ransom* [Delft University of Technology]. ⟨http://resolver.tudelft.nl/uuid:a3594946-b09c-4b0f-b3d6-abe0222a03d0⟩.
Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly: Management Information Systems, 22*(4), 441–464. https://doi.org/10.2307/249551
Thakur, S., Chaudhari, S., & Joshi, B. (2021). Ransomware: Threats, identification and prevention. *In Cyber Security and Digital Forensics*. wiley,. https://doi.org/10.1002/9781119795667.ch16
Tripathi, M., & Mukhopadhyay, A (2022). Does privacy breach affect firm performance? An analysis incorporating event-induced changes and event clustering. *Information & Management, 59*(8), Article 103707. https://doi.org/10.1016/j.im.2022.103707
Tsen, E., Ko, R. K. L., & Slapnicar, S. (2022). An exploratory study of organizational cyber resilience, its precursors and outcomes. *Journal of Organizational Computing and Electronic Commerce, 32*(2), 153–174. https://doi.org/10.1080/10919392.2022.2068906
Wang, J., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution. *MIS Quarterly, 39*(1), 91–112. ⟨https://www.jstor.org/stable/26628342⟩.
Wei, X., Zhang, Z., Zhang, M., Chen, W., & Zeng, D. D. (2022). Combining crowd and machine intelligence to detect false news on social media. *MIS Quarterly, 46*(2), 977–1008. https://doi.org/10.25300/MISQ/2022/16526
Weill, P., & Woerner,S. L. (2018). Is Your Company Ready for a Digital Future? MIT SLOAN MANAGEMENT REVIEW, 59(2), 21–25.
Weixun Li, W., Chung Man Leung, A., & Yue, W. T. (2023). Where is it in information security? the interrelationship among it investment, security awareness, and data breaches. *MIS Quarterly, 47*(1), 317–342. https://doi.org/10.25300/MISQ/2022/15713
Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management, 66*, Article 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520
Wunderlich, P., Veit, D. J., & Sarker, S. (2019). Adoption of Sustainable Technologies: A Mixed-Methods Study of German Households. *MIS Quarterly, 43*(2), 673–691. https://doi.org/10.25300/MISQ/2019/12112
Yahav, I., Shmueli, G., Mani, D., Baesens, B., Bapna, R., Marsden, J. R., Vanthienen, J., & Zhao, J. L. (2016). Tree-based approach for addressing self-selection in impact studies with big data. *MIS Quarterly: Management Information Systems, 40*(4), 819–848. ⟨http://www.misq.org⟩.
Yoo, C., Goo, J., & Rao, R. (2020). Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness. *MIS Quarterly, 44*, 907–931. https://doi.org/10.25300/MISQ/2020/15477
Young, S. (2021). When ransomware strikes, what's your recovery plan? *Network Security, 2021*(7), 16–19. https://doi.org/10.1016/S1353-4858(21)00077-5
Yuryna Connolly, 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
Zhang, H., Xiao, X., Mercaldo, F., Ni, S., Martinelli, F., & Sangaiah, A. K. (2019). Classification of ransomware families with machine learning based onN-gram of opcodes. *Future Generation Computer Systems, 90*, 211–221. https://doi.org/10.1016/j.future.2018.07.052
Zhuang, Y., Choi, Y., He, S., Leung, A. C. M., Lee, G. M., & Whinston, A. (2020). Understanding security vulnerability awareness, firm incentives, and ICT development in Pan-Asia. *Journal of Management Information Systems, 37*(3), 668–693. https://doi.org/10.1080/07421222.2020.1790185
Zuhair, H., Selamat, A., & Krejcar, O. (2020). A multi-tier streaming analytics model of 0-day ransomware detection using machine learning. *Applied Sciences, 10*(9). https://doi.org/10.3390/a