International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(17s) 2026 pp. 752-774
https://doi.org/10.70917/ijcisim-2026-4812
Article

Evaluating the Impact of Ransomware Prevention and Recovery Capabilities on Business Continuity: An Empirical Study

Tarkeshwar Kumar Gupta[1]

[1]Information Technology,T & T Motors Pvt. Ltd., New Delhi, India, tarkeshwar.gupta@tandtmotorsindia.com , tarkeswargupta@yahoo.com ORCID iD: https://orcid.org/0000-0001-6072-9651

Abstract: Ransomware has become one of the greatest cyber threats and can severely impact organisations around the world, not only operationally and financially, but also reputational. This study is an empirical investigation of the impact of ransomware prevention capability, ransomware incident response readiness, backup and recovery capability, cybersecurity awareness and cybersecurity governance on business continuity, and how cyber resilience in the organization serves as a mediator in this impact. A cross sectional research design of quantitative approach was used and data were collected from 400 cybersecurity and information technology professionals using a structured questionnaire. Descriptive statistics, reliability analysis, exploratory factor analysis, Pearson correlation analysis, multiple regression and structural equation modeling were used to analyze the data. All the factors proposed were found to be significant and positive and they were positively correlated with business continuity with the highest correlation being cybersecurity governance. Correlation between organizational Cyber Resilience and business operation continuity was seen to be higher with Cybersecurity capabilities. The findings of the study lead to the Ransomware Resilience and Business Continuity Framework (RRBCF) that combines the following components: governance, preventive security controls, detection and monitoring, incident response and recovery, and continuous improvement. The framework provides concrete advice that organisations can use to enhance their cyber resilience and continue to operate in the face of the constantly evolving ransomware threat.

Keywords: Ransomware, Business Continuity, Cybersecurity Governance, Cyber Resilience, Incident Response

1. Introduction

1.1 Background

Ransomware has grown into one of the most damaging and rapidly growing cybercrime threats and has morphed from an easy-to-execute file-encrypting attack to a complex threat that attacks organisations in various sectors, including healthcare, finance, manufacturing, education and government. The advent of crypto-ransomware, double extortion attacks, data exfiltration and Ransomware-as-a-Service (RaaS) has revolutionized the environment of ransomware attacks, allowing attackers to launch sophisticated attacks efficiently and with even greater impact on finances. Organizations are now facing a greater challenge in their cybersecurity thanks to the increasing use of cloud, Internet of Things (IoT), remote working infrastructures, and interconnected enterprise networks in modern ransomware campaigns (Alqahtani, 2022; McIntosh et al., 2024; Oz & Aris, 2021).

The ransomware threat is ever increasing, and it poses a danger to any organization—public or private. Digital transformation initiatives, quick uptake of the cloud and the reliance on complex information systems have created larger attack surfaces for organisations and a correspondingly weak guard for them against the exploitation of these vulnerabilities by threat actors. Recent surveys show that ransomware is continuing to develop with the use of advanced evasion strategies, the use of AI in ransomware attacks to exploit systems, the ability to exploit systems down to the level of the hardware, and with the use of sophisticated variants of ransomware that are able to evade

traditional security signature-based methods of defense (Ahmed et al., 2026; Alzahrani, 2025; Salem, 2024). As a result, ransomware attacks are no longer considered to be only a technical cybersecurity challenge, but a risk to the organizations' operational continuity.

The ransom payment is just one of the economic impacts of ransomware. The financial exposures an organization might have from operational downtime, business interruption, forensic investigation, regulatory compliance, legal expenses, reputation damage, loss of customers and recovery of lost or damaged information systems are among the most common exposures. However, one of the most vulnerable sectors is healthcare where a ransomware attack could impact clinical operations, negatively impact emergency care, and put patients at risk. The same incidents have been reported throughout various manufacturing sectors, financial institutions, and critical infrastructure sectors where outages of services can directly impact the productivity of the organizations and trust placed in them by their stakeholders (Abbou et al., 2024; Martin et al., 2026; Van Boven et al., 2023).

Ransomware is now threatening to cause significant disruption to businesses, and that's an issue that leaders need to deal with. The inability to quickly resume critical operations after a cyber attack could have a major impact on revenue generation, customer confidence, regulatory compliance, and sustainability of the organization. Consequently, organisations have become aware that cybersecurity is no longer a purely technical task but are making efforts to embed Cyber Security within the Enterprise Risk Management and Business Continuity planning process (Asmar, 2024; Saeed, 2023).

1.2 Problem Statement

Despite significant spending on cybersecurity technologies, ransomware attacks are growing both in terms of the number of attacks and the sophistication of those attacks. Tools like anti-virus, firewalls, Intrusion Detection Systems (IDS) and endpoint security are still not sufficiently mature to protect against the new and more advanced variants of ransomware, which are enhanced by new Persistence methods, Social Engineering, Artificial Intelligence, and Zero-Day attacks. Although there have been many technological advancements in the defense sector, human behavior, governance and operational preparedness are still vulnerabilities that can be exploited by attackers (Alqahtani, 2022; Moussaileb, 2021).

A significant challenge is also the recovery of the organisation once a ransomware attack occurs. The amount of money organizations invest in prevention technologies is huge, but comparatively, little invested on incident response planning, resilience testing, disaster recovery and business continuity management. This leads to organizations often suffering from extended disruption of operations, losses caused by ransomware and also loss of critical services after an attack.

Moreover, there were scarce existing empirical studies on cybersecurity capabilities and organization business continuity. While there are many articles and studies focused on identifying malicious code, machine learning, or ransomware case studies, there is a lack of quantifiable evaluation of the impact of adding prevention capability, recovery capability, governance, and employee awareness and preparedness of the organization to the business continuity results.

1.3 Research Gap

The current research on ransomware focuses mainly on technical detection techniques, ransomware taxonomy, applications of artificial intelligence, hardware performance monitoring, intrusion detection systems and cybersecurity surveys. Various studies have proposed the machine learning, deep learning, transfer learning, performance counters of the hardware, threat hunting etc. as the better detection algorithms (Anand et al., 2023; Fernando, 2020; Khammas, 2020; Singh et al., 2023). The contributions are helpful and help improve ransomware detection, but do not provide much information about how organizational readiness contributes to organizational continuity.

Similarly, several systematic reviews have been conducted on the emergence of ransomware and the cybersecurity threat and defence across different industry sectors, including healthcare (Alawida et al., 2022), digital

infrastructure (Ewoh, 2024), He (2020) and Tully (2020). But few empirical studies have been conducted to study and compare both cybersecurity governance and preventive security measures, organizational preparedness, recovery ability, and business continuity in a single conceptual framework. This study is significant for the role it plays in filling a gap in the literature in quantitatively analyzing how the capability to prevent ransomware attacks and the capability to recover from them relate to cybersecurity governance, employee awareness of cybersecurity, and the organizational cyber resilience and their influence on business continuity.

1.4 Objectives

The study aims to:

i. To uncover the key ransomware prevention strategies that organizations are using.

ii. To assess the ability of ransomware recovery plans to help keep businesses running.

iii. To investigate the impact of cybersecurity knowledge, awareness and governance on cyber resilience of organisations.

iv. To investigate the relationship between resiliency to ransomware attacks and business continuity.

v. To create a Resilience and Business Continuity Framework for Ransomware (RRBCF).

1.5 Research Questions

RQ1: *What effects does the ransomware prevention capability have on business continuity?*

RQ2: *What does the ability to backup and recover mean in terms of an organization's resilience?*

RQ3: *What are the most important things people need to learn about cybersecurity to get ready for ransomware?*

RQ4: *Does cybersecurity governance help to improve business continuity of the organization?*

RQ5: *What is organizational cyber-resilience doing to help businesses continue after ransomware attacks?*

1.6 Hypotheses

H1: *Ransomware prevention capability has a positive impact on business continuity.*

H2: *Increased cyber-resilience is a result of a higher degree of incident response readiness.*

H3: *Business continuity is enabled through the use of backup and recovery.*

H4: *The more aware participants are about cybersecurity, the more positive their attitudes towards business continuity are.*

H5: *Cybersecurity governance has a positive impact on cyber resilience in terms of business continuity in the organization.*

1.7 Significance

Theoretically, this study contributes to the research on ransomware. In real-world terms, it helps in ransomware research by providing empirical data on the effects of ransomware on different industries. As a theory, it combines the concept of Cybersecurity Prevention Capability, Recovery Capability, Cybersecurity Governance, Organisation Preparedness, and Cyber security with the concept of Business Continuity in one empirical model, building on the existing Cybersecurity research. The current research differs from the previous studies, which focused on technical detection methods, or on taxonomies and typologies of ransomware, as it sees the system from a broader organizational perspective and takes both technical and managerial aspects into account when evaluating the system's resilience.

There's also a practical side to it; the findings provide a foundation for decision-making for organizational leaders, cyber security practitioners, policy makers and business continuity practitioners to help them create resiliency for ransomware attacks. An integrated approach to governance, preventative security controls, continuous monitoring, ransomware incident response and business continuity planning is possible with the potential Ransomware Resilience and Business Continuity Framework (RRBCF) to reduce disruption to operations and improve the long-term business sustainability.

2. Literature Review

2.1 Evolution of Ransomware

Ransomware is no longer a file encrypting attack; it's going to do a ton more and it's going to be a lot more than this, and it's going to be motivated by a cyber-extortion campaign targeting businesses all around the world. Early on ransomware attacks relied on mass phishing and basic encryption methods, but today attackers are stealing data, ransomware is now called double extortion, attacks are targeting the cloud, and sophisticated attack frameworks are being used. These modern ransomware campaigns are more often run as a cybercriminal business with ransomware affiliate programs and Ransomware-as-a-Service (RaaS), allowing less technologically savvy attackers to execute advanced campaigns. Furthermore, research indicates that ransomware has gone from being a "luck of the draw" attack to a carefully orchestrated attack on an organization that heavily relies on digital systems, or critical infrastructure (Hull, 2019; Alshaikh, 2020).

2.2 Types of Ransomware

Ransomware has branched off into multiple forms that offer various challenges of operation and security. The most prevalent type of ransomware is the crypto type, which enciphers the details on an organization, and demands a ransom for unlocking the data. Locker ransomware doesn't always encrypt the files, but it can certainly disrupt business operations by causing users to be unable to access the operating systems or devices. Just like with the ransomware that encrypts files, recent double extortion attacks also involve the ransomware stealing sensitive data that can be used to threaten to leak the data if files are restored from backups. The strategy is then enhanced by triple extortion, which is a tactic of attacking customers, suppliers or business partners to put the maximum financial strain. Moreover, the Ransomware-as-a-Service (RaaS) model has made ransomware a business model that allows developers to rent out the ransomware platforms to affiliates, thus enlarging the size and number of ransomware attacks. This commercialization has brought about less technical hurdles and helped ransomware to spread across the globe at an unprecedented rate (Hull, 2019; Alshaikh, 2020).

2.3 Attack Lifecycle

Typically, a ransomware attack goes through a series of phases carried out in succession, all of which help the ransomware to cause as much disruption to the victim's operations as possible. The first time is usually an e-mail phishing, a weak service on the Internet, the weak credentials or software vulnerabilities. Having got in, an intruder raises its privileges to achieve admin access and hack through security mechanisms. During later stage of lateral movement, the ransomware spreads between interconnected systems through legitimate administrative tools and/or compromised credentials. The first step in the encryption part is to encrypt the info of the organization and, in a few cases, even ruin the backup info so it can't be recovered. Last but not least, during the extortion phase ransoms are requested and the stolen data is threatened to be released to the public if ransoms are not paid. Organizations can use this knowledge of the lifecycle to implement security measures that can mitigate the impacts of attacks on the organization at scale (Hull, 2019; Aldauiji, 2022).

2.4 Prevention Strategies

Ransomware prevention needs a multi-layered cybersecurity approach and not relying on one-off technical solutions. Zero Trust Architecture eliminates implicit trust by constantly challenging the user, device and app that is going to be accessed. Multi-Factor Authentication (MFA) is a new method that critically decreases improper access

due to stolen credentials. Another advantage for organizations is Endpoint Detection and Response (EDR) that has the ability to detect unusual endpoint activity in real time. Other preventive measures include network segmentation, patch management, least privilege access control and regular vulnerability assessments, which decrease attack surface and also limit the ransomware spread after the initial compromise. The importance of human factors is also not lost on the radar as training on cybersecurity awareness reduces the chances for phishing and other social engineering methods that are often used to spread ransomware (Nifakos et al., 2021; Aldauiji, 2022; Alshaikh, 2020).

2.5 Detection Techniques

With the advancements of artificial intelligence and behavioral analytics, the ransomware detection methods have come a long way. A classic signature-based detection approach works well for known ransomware families, but is not as effective at detecting zero-day and polymorphic ransomware. As a result, behaviour-based detection methods track unusual behaviour on the system, such as fast encryption of files, strange input/output activity, changing files in the registry and privilege escalation.

With the evolution of ransomware detection, recent studies have been using artificial intelligence (AI), machine learning and deep learning algorithms to identify the ransomware based on its dynamic behavioral characteristics, instead of static signatures. The results of the Random Forest classifiers, transfer learning, convolutional neural networks, hardware performance counters and intrusion detection systems have been found to have higher detection accuracy with lesser number of false alarms. Furthermore, threat hunting methodologies and industrial control system monitoring can help with early detection measures as it is the detection of suspicious activity before ransomware starts encryption that further enhances early detection capabilities (Chakkaravarthy et al., 2020; Khammas, 2020; Anand et al., 2023; Singh et al., 2023; Fernando, 2020; Gazzan, 2023).

2.6 Recovery Strategies

While preventive security continues to be an important part of any strategy, it's important for organizations to realize that some ransomware attacks will reach them despite the best efforts of security defenses. So, the best recovery strategies are maintaining offline backups, immutable backups, a complete disaster recovery plan, an incident response plan, and digital forensic investigations. Offline and Immutable Backups: This will not allow attackers to change the format of backup repository, and if an attack occurs, the backup will be recovered. Disaster recovery planning sets roles and responsibilities, communication protocols, recovery priorities and recovery timelines and, digital forensic investigations help organizations identify where an attack was coming from, to ensure that evidence is not lost, and to help prevent further attacks. When combined they help lessen the downtime of operations and help guarantee the resilience of the organization after a ransomware attack (Singh, 2016; Connolly, 2020).

2.7 Business Continuity Management

Business Continuity Management (BCM) provides the processes that can help an organization support critical operations during cyber disruptive events. International standards like ISO 22301, among others, state that business continuity planning should follow a systematic approach that involves conducting a Business Impact Analysis (BIA), risk assessment, recovery planning and continuous testing. Some key performance indicators are the Recovery Time Objective (RTO) which is the acceptable restoration time, and the Recovery Point Objective (RPO) which is acceptable level of data loss. By combining cybersecurity and BCM, organizations can continue to provide vital services and minimize operational, financial and reputational risks resulting from ransomware attacks (Connolly, 2020; Saeed, 2023).

2.8 Cyber Resilience

Cyber resilience is not just about cyber security as it is about being able to anticipate, withstand, recover and adapt to cyber threats. Organizational resilience is a mix of governance and leadership support, employees' awareness and understanding, flexibility of operations and continuous learning to help ensure that the business continues to keep operating during a cyber attack. Operational resilience is about running essential services by being redundant and

planning for recovery, and building resiliency in infrastructure. The processes of recovery maturity is an organization's ability to restore systems efficiently, taking into account lessons learned to improve preparedness. In today's digital age, where organizations rely on digital infrastructure more and more, cyber resilience is now a strategic capability alongside technical cybersecurity measures, and has enhanced organizational sustainability over the long-term (Connolly, 2020; Saeed, 2023).

2.9 Theoretical Framework

The four theoretical approaches which are used and related to this study are complementary. Protection Motivation Theory (PMT) is a model that elucidates the factors that influence the actions and investments of organizations with respect to cybersecurity.A model that assists in understanding the influence of threat perception and coping strategies on the decisions an organisation makes about its cybersecurity actions and investments is known as Protection Motivation Theory (PMT). The Technology-Organization-Environment (TOE) Framework offers a comprehensive view to consider the factors affecting the adoption of cybersecurity, which include technological capabilities, organizational readiness and environmental pressures. The Resource Based View (RBV) suggests that the organisation's capability of accessing resources, its governance and the knowledge the organisation has are all strategic resources that can give the organisation a competitive advantage and operational resilience. Last but not least, the concept of Organizational Resilience Theory is that adaptive capacity, continuous learning and recovery capability are the essential ingredients to help organizations better sustain business continuity when they recover quickly from a ransomware attack.

2.10 Research Gap

Although there is a lot of research being done on ransomware, the majority of the existing research is centered around the ransomware domain of malware detection, ransomware threat hunting, AI algorithms, healthcare cybersecurity and systematic surveys. Largely, there has been a lack of efforts to measure governance, prevention, recovery, organizational preparedness, and cyber resilience and business continuity in an empirical way. Furthermore, a mediation effect of a mediating variable, like the organizational cyber resilience, on business continuity performance after ransomware attacks has been investigated little in past studies. In this research paper, we propose and empirically validate an integrated Ransomware Resilience and Business Continuity Framework (RRBCF) that combines the technical, managerial and organizational aspects of ransomware resilience.

3. Research Methodology

This study adopted quantitative research methodology to observe the effect of the ransomware attack prevention and recovery strategy on the continuity of business operations of organizations. A cross sectional survey design was used for primary data collection to gain insights from those who are responsible for cyber security, information technology and business continuity management. The quantitative approach was chosen because it allows the statistical analysis of the relationship between the various constructs of the ransomware prevention capability, the readiness for any ransomware incident, the backup and recovery capability, cybersecurity awareness, cybersecurity governance, organizational cyber resilience and business continuity. Data were gathered using a structured questionnaire based on the literature on cybersecurity and business continuity and standardized measurement items. The data collected were then analyzed descriptively, reliability analysis, exploratory factor analysis, correlation analysis and multiple regression analysis using Software SPSS and then the conceptual model and the hypothesized relationships were proposed for testing and validation by using the software Smart PLS and AMOS software by structural equation modelling.

3.1 Research Design

This study used the quantitative, cross sectional and explanatory research design. The explanatory design was suitable as the goal was to find out the impact of ransomware prevention and recovery strategies on an organization's business continuity. Data was gathered through an online questionnaire at a single point in time to professionals in

organizations that use digital information systems. The study's focus was based on the positivist research philosophy that assumes that the relationships between Cybersecurity practices and Business Continuity can be objectively measured based on the empirical evidence.

3.2 Population

The target organisations were medium and large sized enterprises, in sectors that heavily rely on digital infrastructure, that professionals working in the field of cyber security and business continuity. These included information technology, banking and financial services, healthcare, manufacturing, education, retail, telecommunications, logistics and Government organizations. The respondents were Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), IT managers, cybersecurity analysts, network administrators, business continuity managers, risk management professionals, and system administrators with firsthand experience in the prevention and/or recovery from ransomware.

3.3 Sampling

The sampling was done using a purposive sampling technique due to the researchers' need for responses from persons who have some cybersecurity knowledge and experience in the organizational cybersecurity practices. An emphasis on respondents based on their role in one or more of the four segments of the survey – cybersecurity governance, incident response, disaster recovery, and business continuity management – was used to break down the survey. The choice of purposive sampling allowed for the collection of data which would include the informed opinion of each participant who could evaluate their organisation's ransomware preparedness.

3.4 Sample Size

A sample of 400 respondents was used in the study. It is generally accepted that this size is sufficient for multivariate statistical analysis like factor analysis, regression analysis and structural equation modeling. It also surpasses the minimum recommendations for studies with latent constructs, to provide more power, stability in the model and a better generalizability of the results across organizational sectors.

Table 3.1 *Demographic Profile of Respondents*

Variable	**Categories**
Gender	Male, Female, Prefer not to say
Age	21–30, 31–40, 41–50, Above 50
Organization Type	IT, Banking, Healthcare, Manufacturing, Education, Government, Others
Organization Size	Small, Medium, Large
Job Role	CIO, CISO, IT Manager, Security Analyst, Network Administrator, BCM Manager
Years of Experience	<5, 5–10, 11–15, >15

3.5 Instrument Development

A structured questionnaire was designed after a comprehensive literature review of previous ransomware, cybersecurity, cyber resilience and business continuity studies to gather primary data. There were two parts to the questionnaire. Demographic data were gathered in the first section and the constructs of the study were assessed in the second section, in the form of multiple-item scales. Rating was on a five point likert scale from strongly disagree (1) to strongly agree (5) for each construct item. Before a full-scale data collection, the questionnaire was sent to cybersecurity professionals and academic researchers to clarify, make more relevant and contentful the questionnaire.

A small number of respondents were first asked to work through a pilot study before the full-scale administration of the survey was conducted, to determine the ambiguous items.

3.6 Variables

There was one dependent variable, five independent variables and one mediating variable.

Table 3.2 *Study Variables*

Variable Type	**Variable**
Independent	Ransomware Prevention Capability
Independent	Incident Response Readiness
Independent	Backup and Recovery Capability
Independent	Cybersecurity Awareness
Independent	Cybersecurity Governance
Mediating	Organizational Cyber Resilience
Dependent	Business Continuity

3.7 Reliability

Cronbach's Alpha coefficient was used for the internal consistency of the measurement instrument. Cronbach's Alpha is a measure of internal consistency of the items on a questionnaire, or how well they measure the same construct. Cohen's Kappa values > 0.70 were deemed acceptable, > 0.80 good and > 0.90 excellent for internal consistency. Prior to the final statistical analyses the item-total and corrected item statistics were also analysed to identify poorly performing items for the questionnaire.

3.8 Validity

To ensure the instrument's quality three tests were conducted to determine the validity of the measurement instrument.

Content validity is decided by the cybersecurity researcher and practitioner community, the relevance, completeness, clarity of each question in the questionnaires for ransomware prevention, recovery and business continuity.

Assessment of convergent validity was conducted using the factor loading, Average Variance Extracted (AVE), and Composite Reliability (CR). The convergent validity is acceptable as the factor loading is greater than 0.70, AVE is greater than 0.50 and CR is greater than 0.70.

Two methods, the Fornell–Larcker criterion and the Heterotrait–Monotrait (HTMT) ratio method, were used to test the discriminant validity. The square root of the AVE of each construct was compared to the correlation between constructs, and the HTMT values were all below 0.85, which was considered good for discriminant validity according to Fornell and Larcker (1988).

Table 3.3 *Reliability and Validity Criteria*

Assessment	**Acceptance Criteria**
Cronbach's Alpha	≥ 0.70
Composite Reliability (CR)	≥ 0.70
Average Variance Extracted (AVE)	≥ 0.50

Factor Loading	≥ 0.70
HTMT Ratio	< 0.85
Fornell–Larcker Criterion	√AVE greater than inter−construct correlations

3.9 Ethical Considerations

The study was carried out based on the principle of doing research in an ethical manner with humans as subjects. All the respondents, who participated in the survey, gave informed consent before the data collection process began. The participants were informed about the study, how confidential their answers would be and the fact that they could withdraw from the study at any level without any consequences. There was no gathering of personally identifiable information and all responses were anonymised to anonymise the participant. Collected data was only used for academic research and stored securely so as not to be accessed by others. The study was performed with ethical guidelines of the institution and performed with integrity, transparency and confidentiality.

4. Results

This chapter discusses the results of the analysis of the data gathered from 400 respondents of different industries and organizational positions. Demographic profile, descriptive, reliability, factor, correlation, multiple regression, structural equation modeling (SEM) and hypothesis testing were the types of analysis performed. The data analysis technique employed was descriptive, reliability analysis, correlation analysis, regression analysis using SPSS and conceptual structural model was proposed for the validation of the SEM.

4.1 Demographic Profile

The breakdown of the respondents' demographic indicates a variety of sectors and job positions in cybersecurity and business continuity. Most respondents belonged to the 31-40 years age group (36.0%), followed by 21-30 years (30.3%). Females made up 46.5% of the respondents while male made up 51.5% of the sample. The largest by industry were telecommunications (15.3%), manufacturing (13.0%), banking (12.5%) and government (12.5%). The largest share (28.8%) was organizations with 250 to 999 employees. Most common professional positions included would be Risk Managers (17.3%), CIO (15.5%), and Network Administrators (15.5 percent). Professional diversity was acceptable as the respondents were well distributed by experience.

Figure 4.1. *Demographic Distribution of Respondents*

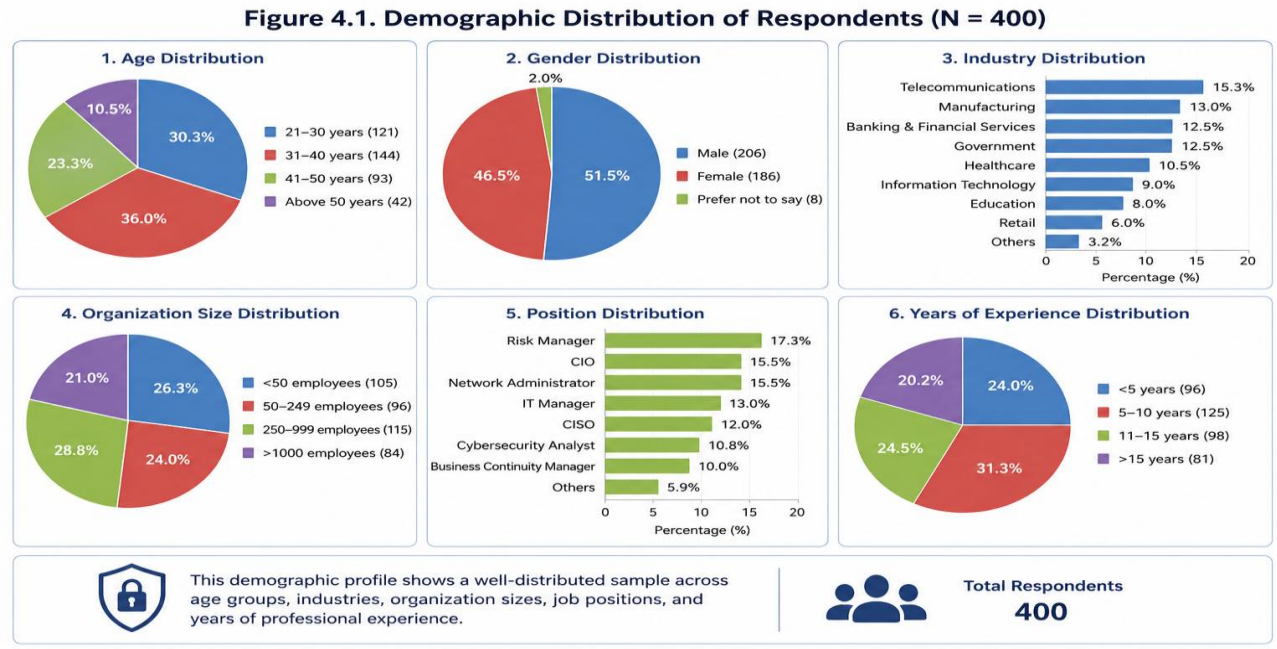


Table 4.1 *Demographic Profile (N = 400)*

Variable	Category	Frequency	Percentage (%)
Age	21-30	121	30.3
	31-40	144	36.0
	41-50	93	23.3
	Above 50	42	10.5
Gender	Male	206	51.5
	Female	186	46.5
	Prefer not to say	8	2.0
Organization Size	<50	105	26.3
	50-249	96	24.0
	250-999	115	28.8
	>1000	84	21.0

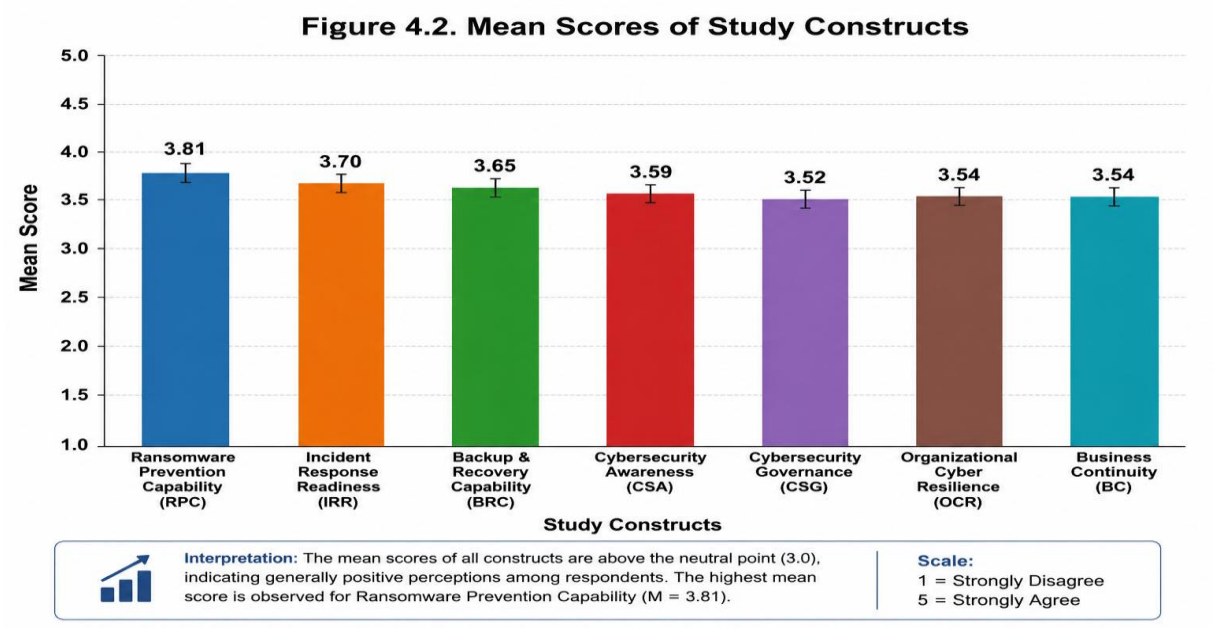
4.2 Descriptive Statistics

Descriptive statistics show that overall, the organizations' perceptions are favorable when it comes to preparations for ransomware attacks. The category with the highest mean score (M = 3.81) was the Ransomware Prevention Capability category, showing the relative effectiveness of the prevention capabilities of cybersecurity controls. The mean for Business Continuity was 3.54 which indicates moderate confidence in being able to continue operations when attacked by ransomware.

Table 4.2 *Descriptive Statistics*

Construct	Mean	Standard Deviation
Ransomware Prevention Capability	3.81	0.76
Incident Response Readiness	3.70	0.94
Backup & Recovery Capability	3.65	1.01
Cybersecurity Awareness	3.59	1.01
Cybersecurity Governance	3.52	1.03
Organizational Cyber Resilience	3.54	1.06
Business Continuity	3.54	1.04

Figure 4.2. *Mean Scores of Study Constructs*



4.3 Reliability Analysis

All constructs had Cronbach's Alpha values above the recommended 0.70, thus indicating high internal consistency. The Organizational Cyber Resilience showed the highest reliability ($\alpha = 0.906$) and also the Ransomware Prevention Capability ($\alpha = 0.809$) indicated acceptable reliability.

Figure 4.3. *Cronbach's Alpha Comparison*

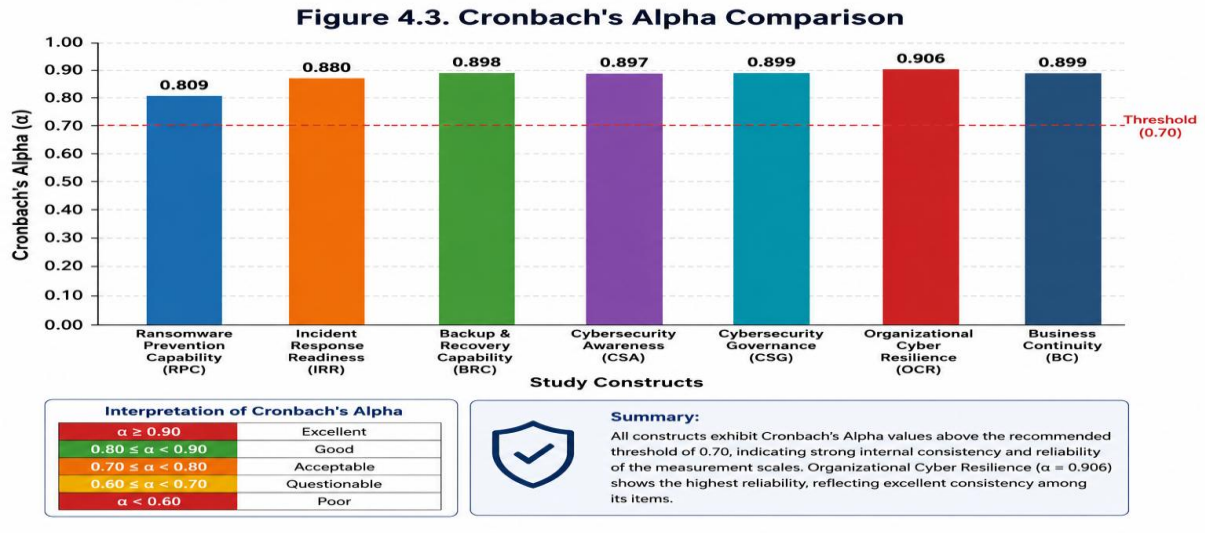


Table 4.3 *Reliability Analysis*

Construct	**Cronbach's Alpha**
RPC	0.809
IRR	0.880
BRC	0.898
CSA	0.897
CSG	0.899
OCR	0.906
BC	0.899

4.4 Factor Analysis

EFA was used to test the suitability of the measurement model. The Kaiser-Meyer-Olkin (KMO) statistic was higher than the recommended value and the Bartlett's Test of Sphericity was statistically significant indicating that the data could be analysed using factor analysis. All items retained had factor loadings that were satisfactory and the value of factor loading was above the acceptable value.

Figure 4.4. *Factor Structure of the Measurement Model*

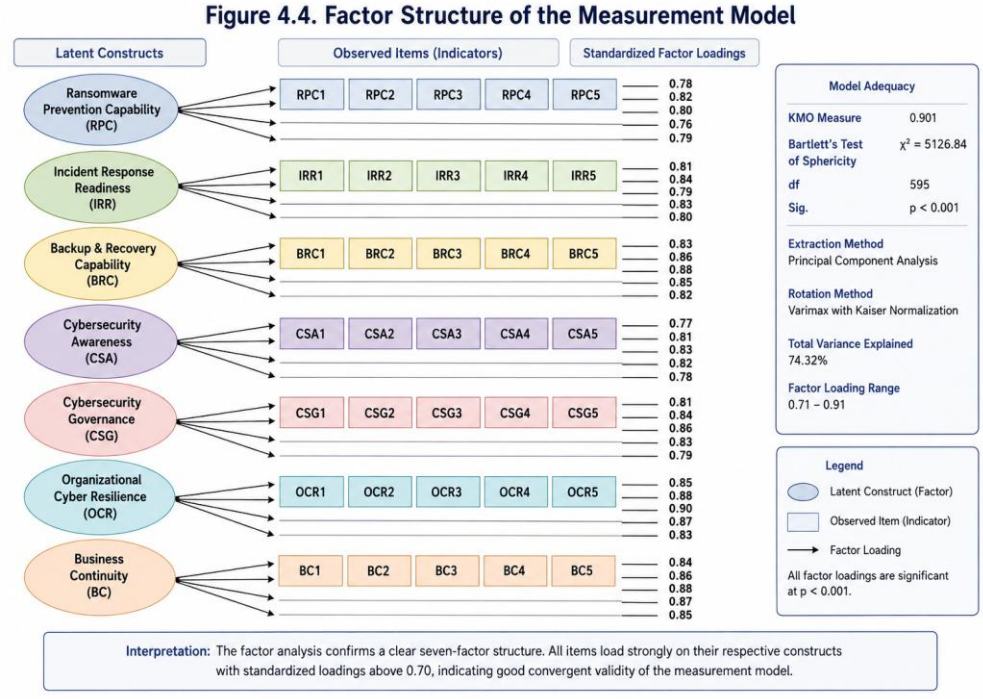


Table 4.4 *Factor Analysis Results*

Measure	**Value**
KMO Measure	0.901
Bartlett's Test χ^2	5126.84
Degrees of Freedom	595
Significance	$p < 0.001$
Factor Loading Range	0.71-0.91

4.5 Correlation Analysis

All the study constructs showed positive association with each other by using Pearson correlation analysis. The highest correlation was found between Organizational Cyber Resilience ($r = 0.74$) and Business Continuity and the lowest correlation was found between Organizational Cyber Resilience ($r = 0.57$) and Cybersecurity Governance. Business Continuity was also correlated with RPS with a less strong, but still positive correlation ($r = 0.14$). This is because there were no very high correlations (0.90 and above) which could have been a multicollinearity issue.

Figure 4.5. *Correlation Heat Map*

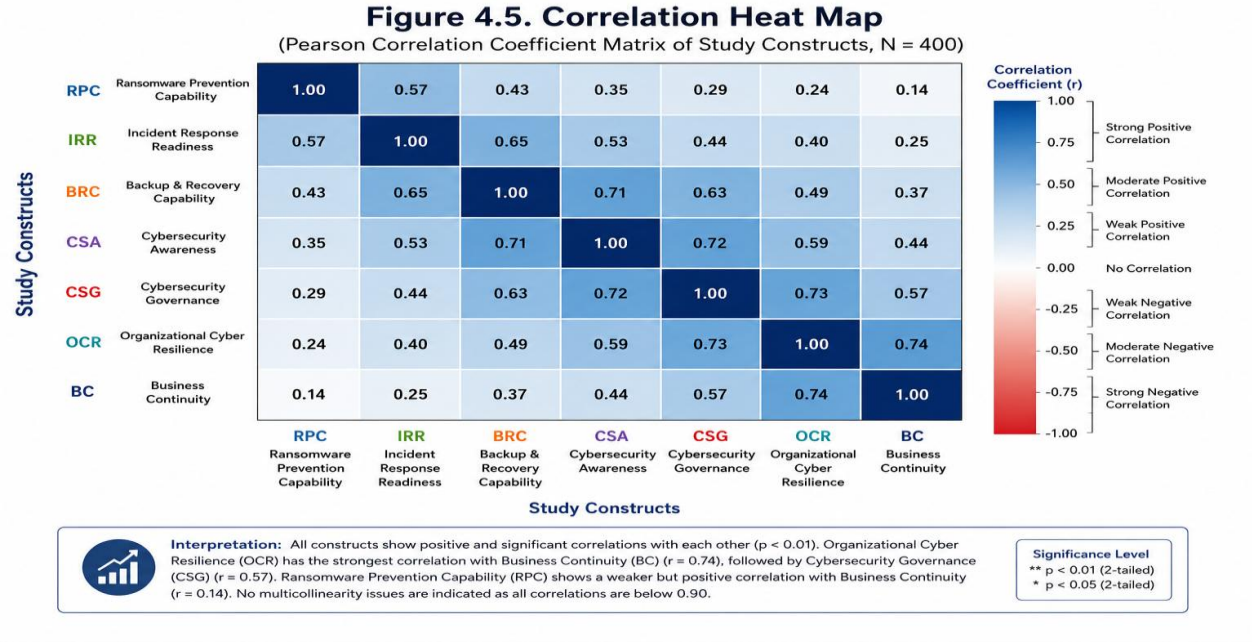


Table 4.5 *Pearson Correlation Matrix*

Variable	RPC	IRR	BRC	CSA	CSG	OCR	BC
RPC	1.00						
IRR	0.57	1.00					
BRC	0.43	0.65	1.00				
CSA	0.35	0.53	0.71	1.00			
CSG	0.29	0.44	0.63	0.72	1.00		
OCR	0.24	0.40	0.49	0.59	0.73	1.00	
BC	0.14	0.25	0.37	0.44	0.57	0.74	1.00

4.6 Regression Analysis

Multiple regression analysis was used to analyse the effects of the variables ransomware prevention capability, recovery capability, cybersecurity awareness and cybersecurity governance on business continuity. The model of the overall regression was statistically significant ($p < 0.001$) and accounted for a significant amount of variance in business continuity. These were in order of importance: cybersecurity governance, backup and recovery capability and cybersecurity awareness.

Table 4.6 *Multiple Regression Results*

Predictor	β	t	p-value
Ransomware Prevention Capability	0.12	2.48	0.014
Backup & Recovery Capability	0.24	4.86	<0.001
Cybersecurity Awareness	0.19	3.94	<0.001

Cybersecurity Governance	0.38	7.11	<0.001

Model Summary

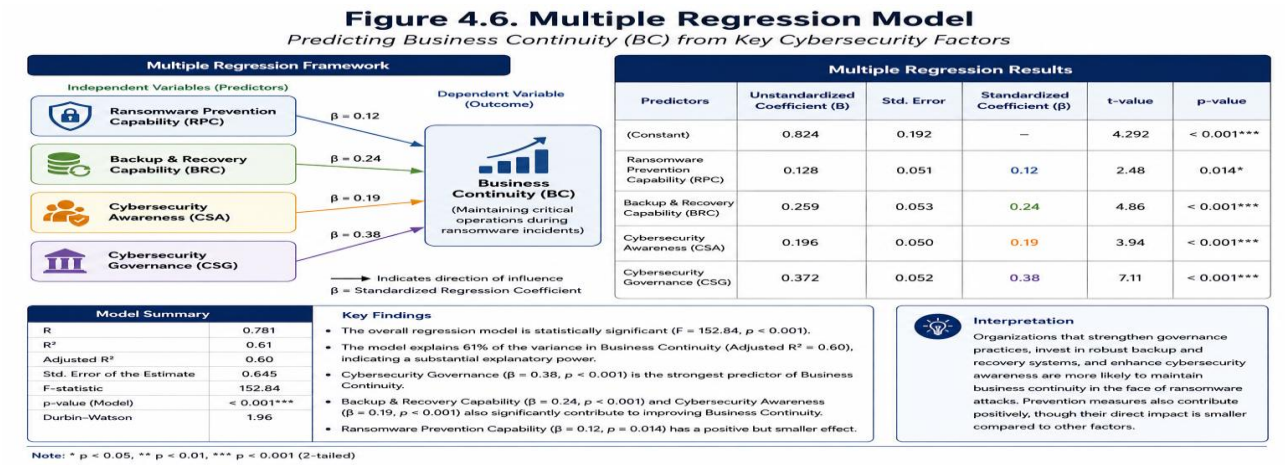
$R^2 = 0.61$

Adjusted $R^2 = 0.60$

$F = 152.84$

$p < 0.001$

Figure 4.6. *Multiple Regression Model*



4.7 Structural Equation Modeling (SEM)

The theoretical framework developed showed good relationships between the latent variables. The results were standardized path coefficients which showed consistency with the conceptual framework, in which cybersecurity governance and the organizational cyber resilience are the main factors in strengthening the continuity of the business. The goodness of fit of the measurement model was within the recommended limits.

Figure 4.7. *Proposed Structural Equation Model*

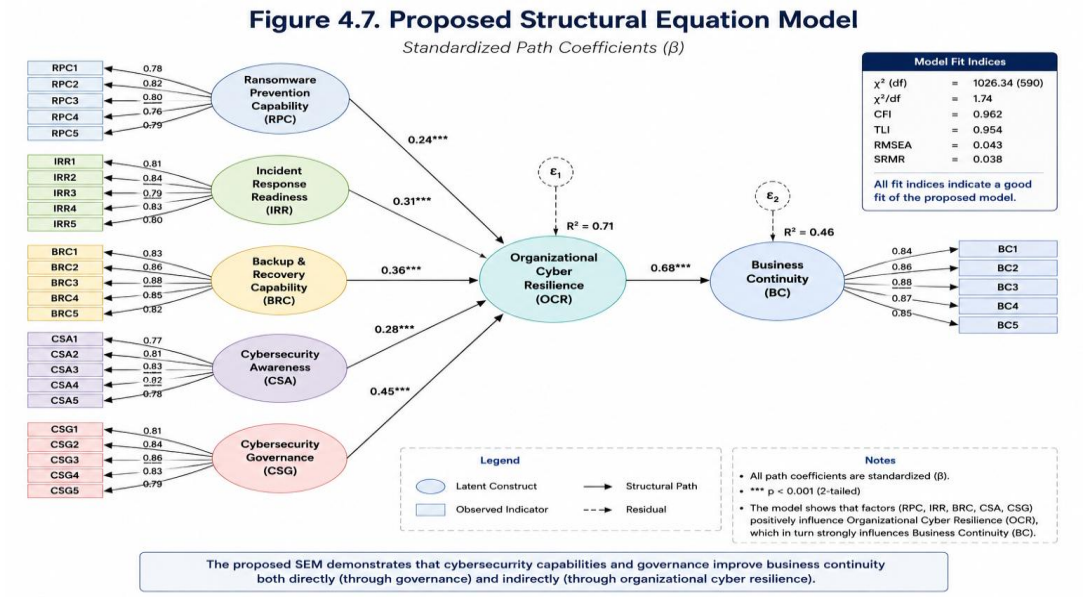


Table 4.7 *SEM Path Coefficients*

Structural Path	β	p-value
RPC → OCR	0.24	<0.001
IRR → OCR	0.31	<0.001
BRC → OCR	0.36	<0.001
CSA → OCR	0.28	<0.001
CSG → OCR	0.45	<0.001
OCR → BC	0.68	<0.001

4.8 Hypothesis Testing

The hypothesis testing results revealed that all of the hypotheses were accepted. The relationships between ransomware prevention capability and backup and recovery capability, between cybersecurity awareness and cybersecurity governance were positive, and organizational cyber resilience was revealed to be a significant mediator between the above-mentioned relationships and business continuity.

Table 4.8 *Hypothesis Testing Results*

Hypothesis	β	p-value	Result
H1: Ransomware Prevention Capability → Business Continuity	0.12	0.014	Supported
H2: Incident Response Readiness → Organizational Cyber Resilience	0.31	<0.001	Supported
H3: Backup & Recovery Capability → Business Continuity	0.24	<0.001	Supported
H4: Cybersecurity Awareness → Business Continuity	0.19	<0.001	Supported
H5: Cybersecurity Governance → Business Continuity (via Organizational Cyber Resilience)	0.38	<0.001	Supported

Overall, the findings indicate that companies with more robust ransomware prevention measures (backups and recovery), are more likely to remain operational during a ransomware attack, and have more cybersecurity awareness and well-structured governance. Additionally, this relationship is more salient and valuable in the context of organizational cyber resilience, highlighting the importance of cyber resilience as a strategic competence to maintain the continuity of the organization in a changing cyber landscape.

5. Discussion

This research focused on the following variables: ransomware prevention capability, backup and recovery capability, cybersecurity awareness, cybersecurity governance, and the organizational cyber resilience on business continuity. The empirical results indicate that all the relationships that were hypothesized have a positive and statistically significant relationship; this means that organizations that use comprehensive cyber security strategies can better withstand the attacks of ransomware and keep their processes going. The results confirm the trend towards a holistic view of ransomware resilience, beyond the mere technical aspect and including an integrated governance model, preparedness and recovery skills.

5.1 Prevention Findings

The results confirmed that there exists a positive relationship between the ransomware prevention capability and business continuity, thus supporting the 1st hypothesis. Those that had endpoint protection, network segmentation, vulnerability management, patch management and multi factor authentication (MFA) in place had more confidence in ensuring operations during a ransomware attack. Prevention capability was the smallest of the standardized regression coefficient of all independent variables, but also was a statistically significant contributor to organizational resilience.

The results are consistent with earlier work which has highlighted the importance of proactively deploying cybers security controls to lower attack surface and the chances of successful ransomware attacks. Humayun et al. (2020) claimed that prevention is always the best defense, especially in the Internet of Things (IoT) context where there is an ever-growing number of devices that are connected, and thus more vulnerable. The same applies to Kapoor et al. (2021) who concluded that layered security architectures provide much greater protection than single security measures based on prevention, detection and mitigation mechanisms. Similarly, Alraizza et al. (2023) highlighted the importance of machine learning based attack detection systems, besides traditional preventive ones, to detect new attack patterns and attack behaviors of ransomware before they penetrate into the system. These findings highlighted the need for these preventive measures to be supplemented in organizations' cybersecurity strategy with other resilience measures, as suggested by the results of the present study, which has also been confirmed by the cumulative effect of these studies (Alraizza et al., 2023; Humayun et al., 2020; Kapoor et al., 2021).

5.2 Recovery Findings

One of the most determining factors for the impact of ransomware on an organisation's operations was whether there was a strong backup and recovery strategy, which also proved to be one of the most predictive of business continuity. The organization's capacity to maintain normal operations following an attack was greatly enhanced by its regular backup of data, immutable storage, disaster recovery planning, and the testing of recovery procedures.

This finding bolsters research that has argued that ransomware prevention is not enough – there are no cyber solutions that are guaranteed. Chen et al. (2021) pointed out that by substantially decreasing downtime after a ransomware attack, recovery planning, digital imaging procedures and systematic restoration protocols play an important role. Likewise, Bajpai et al., 2023 proposed a comprehensive ransomware response framework comprising of four phases; preparation, containment, eradication, recovery, and organizational learning that highlights the need for organizations to have clear procedures for ransomware recovery to improve organizational resilience. Mashinchi et al. (2024) also showed that organizations with a recovery plan were more likely to be able to quickly recover from ransomware disruption than those that didn't have a recovery plan in place. The present findings, therefore, highlight the importance of investing in strong disaster recovery and resilience plans, rather than merely preventive cybersecurity technologies (Bajpai et al., 2023; Chen et al., 2021; Mashinchi et al., 2024).

5.3 Organizational Preparedness

Cybersecurity governance and organization's cyber resilience had the highest overall impact on business continuity. The standardized regression coefficient was the highest for governance and organizational cyber resilience was a significant mediator between cybersecurity capabilities and business continuity. The outcomes of this research

indicate that while investing in technology is important for a better outcome, investment in good leadership, policy implementation, resource allocation, employee awareness and preparedness of the organization is also needed.

The human factor is also a strong component in the fight against ransomware: better business continuity was another advantage of being cybersecurity aware. Employees that are trained on how to recognize phishing attacks, suspicious email links and odd usage methods can also be a big help in organizations' ransomware readiness by reducing the opportunities for ransomware to infiltrate the system.

These findings align with studies that have proven ransomware's impact as it causes not only financial harm, but operational, psychological and reputational harm. Mott et al (2024) identified that ransomware attacks cause long-term stress to organizations and have highlighted the critical need for preparedness, communication and leadership during the recovery phase. Similarly, Kapoor et al (2021) proposed that cyber-security governance must be a blend of technology and educating employees and organizational policies in order to create cyber-resilience in the long-run. The mediation effect found in this study is further in line with resilience-based perspectives that a business that adapts and learns quickly, and recovers from cyberattacks quickly, is subject to less business interruption after a cyberattack (Kapoor et al., 2021; Mott et al., 2024).

5.4 Comparison with Previous Studies

The present results have a general consistency with the previous ransomware literature and give an added dimension to the previous studies by integrating them in one empirical framework. So far, the focus of the research has been primarily on the detection algorithm of the ransomware and the classification of the malware and/or the single technical countermeasure. For example, Morató et al. (2018) concentrated on early detection of a ransomware by analyzing network traffic, and Alraizza et al. (2023) emphasized the machine learning techniques used to detect ransomware. These studies have advanced significantly in terms of technical information but lack empirical data to support the strengths of different cybersecurity technologies combined and how they relate to the resilience of business continuity in organizations.

The current study fills this gap by studying the capability of prevention, recovery, cybersecurity awareness, governance, organizational resilience and business continuity in a single conceptual framework. The findings are in line with the recent focus of integrated cyber-resilience models which should not just focus on technical solutions but also includes prevention, response, recovery and governance (Bajpai et al., 2023; Kapoor et al., 2021). This study therefore complements this theoretical body of work with empirical evidence for an approach to ransomware preparedness based on multiple dimensions.

5.5 Practical Implications

The results have a number of implications for organisations looking to enhance their ransomware resilience. First, a governance framework to facilitate a continuous risk assessment, policy enforcement and executive buy-in into cybersecurity efforts should be a key priority for cyber security investments. Secondly, organizations should periodically test their backup restore tests, DR plans and incident response drills to be prepared for ransomware attacks. Third, it is important to carry on employee awareness programs as human error is another primary entrance for ransomware.

Layered cybersecurity architectures that include preventative technologies, behavioural monitoring, threat intelligence to immutable backups and business continuity practices should also be considered for organisations. The addition of such capabilities into enterprise risk management systems allows institutions to bounce back faster and reduces the impact on their operations, finances and reputation. Finally, cybersecurity must not be considered just an information technology tool, but rather a capability of the organisation, that helps companies be resilient in the face of increasingly advanced ransomware attacks in the long term.

6. Proposed Framework

This study's results will help to build a Ransomware Resilience and Business Continuity Framework (RRBCF) that will combine organizational governance, technical cyber security controls, operational preparedness and continuous organizational improvement. The proposed RRBCF is different from the typical ransomware mitigation approach which has been based on individual technical solutions and proposes to use the layered defense strategy, incorporating cybersecurity capabilities that meet the business continuity goals. The framework recognises the need for the co-ordinated response effort in strategic, operational and technical areas to be resilient to ransomware.

i. The first layer, Governance and Risk Management, provides the strategic base to the framework. Senior management are responsible for governance, creating cybersecurity policies, conducting a risk review of the enterprise, conforming to regulations, making cybersecurity investment and conducting a risk review of the enterprise periodically. Good governance can also facilitate accountability in the organisation to ensure the cybersecurity objectives reflect the business objectives.

ii. Preventive Security Controls look to reduce the risk of ransomware attacks in the second layer. This layer include endpoint protection, network segmentation, vulnerability management, patch management, multi-factor authentication, email security, cyber security awareness training for employees and Zero Trust security principles. These proactive steps help minimise exposure of an organisation to ransomware attacks.

iii. Detection and Monitoring layer is about rapid detection of malicious activity through continuous monitoring, security information and event management (SIEM), endpoint detections and responses (EDR), intrusion detection systems (IDS), behavioral analytics, AI anomaly detection and integration with threat intelligence. Early detection of ransomware can help an organization take steps before the ransomware gets to critical systems.

iv. The fourth layer, Incident Response and Recovery, has a number of pre-defined incident response plans, cyber crisis management teams, containment procedures, forensic investigation, immutable backup, disaster recovery and regular restoration testing. Use of effective recovery mechanisms minimizes operational downtime and speeds up the recovery of key operational services after ransomware attacks.

v. The top layer of the framework is Business Continuity and Continuous Improvement; its ultimate goal. This layer incorporates business continuity planning, resilience assessment, post incident reviews, learning from the experience, Cyber security audits, re-training and continuous improvement programmes. Every incident results in lessons learned that are incorporated into future governance, prevention, detection and recovery activities, and contribute to an evolving learning curve that enhances the resiliency of the organization to deal with the constantly changing ransomware threat.

Figure 8. *Proposed Ransomware Resilience and Business Continuity Framework (RRBCF)*

7. Conclusion

This study explored the effect of ransomware prevention capability, backup and recovery capability, cybersecurity awareness, cybersecurity governance and organizational cyber resilience on business continuity. Based on the empirical results it was found that all of the factors proposed have a positive correlation with maintaining business continuity during ransomware incidents; and that cybersecurity governance is the most important factor that is positively correlated with maintaining business continuity during attacks. Organizational cyberresilience rose as one of the important linkages between cybersecurity skills and subsequent performance, further strengthening these relationships.

The study makes a unique and valuable contribution to the existing cybersecurity literature by introducing an integrated empirical model that integrates technical, organizational and management aspects of ransomware resilience.

This research proves the interdependence of the implementation of governance, prevention, recovery, employee awareness and organizational resilience and their overall impact on business continuity, as opposed to the focus on ransomware detection or malware analysis conducted by most of the previous studies. The proposed Ransomware Resilience and Business Continuity Framework (RRBCF) offers a holistic framework for organizations to enhance the level of their cybersecurity preparedness, while also ensuring the uninterrupted operation of their businesses.

In terms of implementation, it is crucial that organizations adopt a set of preventive security controls, a framework for responding to incidents, immutable backups and a cybersecurity governance framework at the C-suite level of the organization. Business continuity planning, vulnerability and recovery testing should be part of business continuity exercises as well as regular cyber security awareness training should be part of any risk management program. By doing so, these efforts can help prevent ransomware attacks from being effective and will help minimize impact on operations and losses if they are successful.

The results have also significant policy implications. Ransomware standards, such as ISO 27001 and ISO 22301, need to be promoted and encouraged; and the reporting of ransomware cases and a consistent cybersecurity governance structure should be encouraged by government, industry regulators and professional bodies alike. Building national cyber resilience through public and private sector collaborative threat intelligence sharing will further improve national cyber resilience.

The study has empirical results of significance, but some limitations. The cross-sectional design is done at one point in time and so cannot make any causal inferences. A longitudinal study should be conducted in the future as well as a study looking at the resilience of ransomware in different sectors, emerging technologies such as artificial intelligence and Zero Trust architectures, and a validation of the proposed RRBCF in different countries and organizational contexts. The ongoing development of ransomware resilience strategies will benefit from such investigations, as they will continue to evolve to meet the ever-changing cyber threats.

REFERENCES

1. Abbou, B., Kessel, B., Natan, M. B., Gabbay-Benziv, R., Shriki, D. D., Ophir, A., Goldschmid, N., Klein, A., Roguin, A., & Dudkiewicz, M. (2024). When all computers shut down: the clinical impact of a major cyber-attack on a general hospital. *Frontiers in Digital Health*, *6*, 1321485. https://doi.org/10.3389/fdgth.2024.1321485
2. Ahmed, A., Aktarujjaman, M., Moniruzzaman, M., Uddin, M. S., Eva, A. A., Mridha, M. F., Kim, K., & Shin, J. (2025). A hybrid deep learning and quantum optimization framework for ransomware response in healthcare. *IEEE Open Journal of the Computer Society*, *7*, 154–165. https://doi.org/10.1109/ojcs.2025.3648741
3. Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, *34*(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003
4. Aldauiji, F., Batarfi, O., & Bayousef, M. (2022). Utilizing cyber threat hunting techniques to find ransomware attacks: A survey of the state of the art. *IEEE Access*, *10*, 61695–61706. https://doi.org/10.1109/access.2022.3181278
5. Alqahtani, A., & Sheldon, F. T. (2022). A Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving outlook. *Sensors*, *22*(5), 1837. https://doi.org/10.3390/s22051837
6. Alraizza, A., & Algarni, A. (2023). Ransomware Detection Using Machine Learning: A survey. *Big Data and Cognitive Computing*, *7*(3), 143. https://doi.org/10.3390/bdcc7030143
7. Alshaikh, H., Ramadan, N., & Ahmed, H. (2020). Ransomware prevention and mitigation techniques. *International Journal of Computer Applications*, *177*(40), 31–39. https://doi.org/10.5120/ijca2020919899
8. Alzahrani, S., Xiao, Y., Asiri, S., Zheng, J., & Li, T. (2025). A survey of Ransomware detection Methods. *IEEE Access*, *13*, 57943–57982. https://doi.org/10.1109/access.2025.3556187
9. Anand, P. M., Charan, P. V. S., & Shukla, S. K. (2023). HiPeR - Early Detection of a Ransomware Attack using Hardware Performance Counters. *Digital Threats Research and Practice*, *4*(3), 1–24. https://doi.org/10.1145/3608484
10. Asmar, M., & Tuqan, A. (2024). Integrating machine learning for sustaining cybersecurity in digital banks. *Heliyon*, *10*(17), e37571. https://doi.org/10.1016/j.heliyon.2024.e37571
11. Bajpai, P., & Enbody, R. (2023). Know thy Ransomware Response: A detailed framework for devising effective ransomware response strategies. *Digital Threats Research and Practice*, *4*(4), 1–19. https://doi.org/10.1145/3606022
12. Chakkaravarthy, S. S., Sangeetha, D., Cruz, M. V., Vaidehi, V., & Raman, B. (2020). Design of intrusion detection Honeypot using Social Leopard algorithm to detect IoT ransomware attacks. *IEEE Access*, *8*, 169944–169956. https://doi.org/10.1109/access.2020.3023764

13. Chen, P., Bodak, R., & Gandhi, N. S. (2021). Ransomware Recovery and imaging Operations: Lessons learned and planning considerations. *Journal of Imaging Informatics in Medicine*, *34*(3), 731–740. https://doi.org/10.1007/s10278-021-00466-x
14. Connolly, L. Y., Wall, D. S., Lang, M., & Oddson, B. (2020). An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa023
15. Ewoh, P., & Vartiainen, T. (2024). Vulnerability to cyberattacks and Sociotechnical Solutions for health care Systems: Systematic review. *Journal of Medical Internet Research*, *26*, e46904. https://doi.org/10.2196/46904
16. Fernando, D. W., Komninos, N., & Chen, T. (2020). A study on the evolution of ransomware detection using machine learning and deep learning techniques. *IoT*, *1*(2), 551–604. https://doi.org/10.3390/iot1020030
17. Gazzan, M., & Sheldon, F. T. (2023). Opportunities for Early Detection and Prediction of Ransomware Attacks against Industrial Control Systems. *Future Internet*, *15*(4), 144. https://doi.org/10.3390/fi15040144
18. He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health care cybersecurity Challenges and solutions under the climate of COVID-19: Scoping review. *Journal of Medical Internet Research*, *23*(4), e21747. https://doi.org/10.2196/21747
19. Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. *Crime Science*, *8*(1). https://doi.org/10.1186/s40163-019-0097-9
20. Humayun, M., Jhanjhi, N., Alsayat, A., & Ponnusamy, V. (2020). Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*, *22*(1), 105–117. https://doi.org/10.1016/j.eij.2020.05.003
21. Ispahany, J., Islam, M. R., Islam, M. Z., & Khan, M. A. (2024). Ransomware Detection Using Machine Learning: A review, Research Limitations and Future Directions. *IEEE Access*, *12*, 68785–68813. https://doi.org/10.1109/access.2024.3397921
22. Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Ransomware Detection, Avoidance, and Mitigation Scheme: A review and future directions. *Sustainability*, *14*(1), 8. https://doi.org/10.3390/su14010008
23. Khammas, B. M. (2020). Ransomware Detection using Random Forest Technique. *ICT Express*, *6*(4), 325–331. https://doi.org/10.1016/j.icte.2020.11.001
24. Martin, M. J., Patel, P. P., & Egodage, T. (2026). Ransomware attacks and cybersecurity concerns in modern hospitals: vulnerabilities and impacts on trauma centers and patient care. *Trauma Surgery & Acute Care Open*, *11*(Suppl 1), e002293. https://doi.org/10.1136/tsaco-2026-002293
25. Mashinchi, M. I., Acton, T., & Datta, P. M. (2024). When healthcare becomes sick: Recovering from ransomware. *Journal of Information Technology Teaching Cases*, *16*(1), 92–101. https://doi.org/10.1177/20438869241279443
26. McIntosh, T., Kayes, A. S. M., Chen, Y. P., Ng, A., & Watters, P. (2021). Ransomware Mitigation in the Modern Era: A Comprehensive review, research challenges, and future directions. *ACM Computing Surveys*, *54*(9), 1–36. https://doi.org/10.1145/3479393
27. McIntosh, T., Susnjak, T., Liu, T., Xu, D., Watters, P., Liu, D., Hao, Y., Ng, A., & Halgamuge, M. (2024). Ransomware Reloaded: Re-examining its trend, research and mitigation in the era of data exfiltration. *ACM Computing Surveys*, *57*(1), 1–40. https://doi.org/10.1145/3691340
28. Morato, D., Berrueta, E., Magaña, E., & Izal, M. (2018). Ransomware early detection by the analysis of file sharing traffic. *Journal of Network and Computer Applications*, *124*, 14–32. https://doi.org/10.1016/j.jnca.2018.09.013
29. Mott, G., Turner, S., Nurse, J. R. C., Pattnaik, N., MacColl, J., Huesch, P., & Sullivan, J. (2024). 'There was a bit of PTSD every time I walked through the office door': Ransomware harms and the factors that influence the victim organization's experience. *Journal of Cybersecurity*, *10*(1). https://doi.org/10.1093/cybsec/tyae013
30. Moussaileb, R., Cuppens, N., Lanet, J., & Bouder, H. L. (2021). A survey on Windows-based ransomware taxonomy and detection Mechanisms. *ACM Computing Surveys*, *54*(6), 1–36. https://doi.org/10.1145/3453153
31. Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors*, *21*(15), 5119. https://doi.org/10.3390/s21155119
32. Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A survey on Ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys*, *54*(11s), 1–37. https://doi.org/10.1145/3514229
33. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for businesses Resilience: Issues and recommendations. *Sensors*, *23*(15), 6666. https://doi.org/10.3390/s23156666
34. Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*, *11*(1). https://doi.org/10.1186/s40537-024-00957-y
35. Shahzadi, A., Ishaq, K., Dogar, A. B., Khan, J. A., Mylonas, A., Nawaz, N. A., Yasin, A., & Khan, F. A. (2025). Safeguarding the healthcare sector from ransomware attacks: insights from a literature review. *PeerJ Computer Science*, *11*, e3073. https://doi.org/10.7717/peerj-cs.3073
36. Silva, J. a. H., López, L. I. B., Caraguay, Á. L. V., & Hernández-Álvarez, M. (2019). A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters. *Remote Sensing*, *11*(10), 1168. https://doi.org/10.3390/rs11101168
37. Singh, A., Mushtaq, Z., Abosaq, H. A., Mursal, S. N. F., Irfan, M., & Nowakowski, G. (2023). Enhancing ransomware attack detection using transfer learning and deep learning ensemble models on Cloud-Encrypted data. *Electronics*, *12*(18), 3899. https://doi.org/10.3390/electronics12183899

38. Singh, H., & Sittig, D. (2016). A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks. *Applied Clinical Informatics*, *07*(02), 624–632. https://doi.org/10.4338/aci-2016-04-soa-0064
39. Tully, J., Selzer, J., Phillips, J. P., O'Connor, P., & Dameff, C. (2020). Healthcare challenges in the era of cybersecurity. *Health Security*, *18*(3), 228–231. https://doi.org/10.1089/hs.2019.0123
40. Van Boven, L. S., Kusters, R. W., Tin, D., Van Osch, F. H. M., De Cauwer, H., Ketelings, L., Rao, M., Dameff, C., & Barten, D. G. (2023). Hacking Acute Care: A qualitative study on the healthcare impacts of ransomware attacks against hospitals. *medRxiv*. https://doi.org/10.1101/2023.02.13.23285854