

Final Project 2

PMG 497

Midocean University

Faculty of Management

Bachelor of Project Management



The Impact of Cyber Resilience Capabilities on Business Continuity in Saudi Organizations

Student name

Mohammed Hani Abdelaal

Final Project - 2

Faculty of Management - Midocean University

Supervisor

Dr. Abdelrehim Nader

Faculty member- Faculty of management- Midocean University

02/08/2026 – Second Trimester 2026

Abstract

Cybersecurity threats can significantly disrupt organizational operations and affect the ability of organizations to maintain business continuity. This study examines the relationship between Cyber Resilience Capabilities and Business Continuity in Saudi organizations, focusing on Threat Detection, Incident Response, Recovery Capability, and Security Awareness. A quantitative cross-sectional research design was adopted, and data were collected through a structured questionnaire using a five-point Likert scale. A total of 384 valid responses were obtained and analyzed using SPSS Version 29. Descriptive statistics, Cronbach's Alpha, Pearson correlation analysis, and multiple regression analysis were employed to evaluate the research variables and hypotheses. The questionnaire demonstrated excellent overall reliability (Cronbach's Alpha = 0.952). The findings revealed a very strong positive and statistically significant relationship between Cyber Resilience Capabilities and Business Continuity ($r = 0.909$, $p < 0.001$). Multiple regression analysis indicated that the four Cyber Resilience dimensions collectively explained 82.8% of the variance in Business Continuity ($R^2 = 0.828$, Adjusted $R^2 = 0.826$). Threat Detection, Incident Response, Recovery Capability, and Security Awareness were all significant positive predictors of Business Continuity. The findings highlight the importance of strengthening Cyber Resilience Capabilities as part of an integrated approach to improving Business Continuity in Saudi organizations.

Keywords: Cyber Resilience, Business Continuity, Threat Detection, Incident Response, Recovery Capability, Security Awareness, Saudi Organizations

Table of Contents

Abstract	3
1. Chapter 1: Introduction	7
1.1. Research Background	8
1.2. Research Problem.....	11
1.2.1. Theoretical Gaps	12
1.2.2. Practical Gaps.....	13
1.3. Research Significance.....	14
1.3.1. At the theoretical level	14
1.3.2. At the practical level	15
1.4. Research Questions	16
1.5. Research Objectives	16
1.6. Research Hypotheses.....	17
1.7. Research Model	18
1.8. Scope of The Study	18
1.9. The Project Structure.....	19
2. Chapter 2: Literature Review.....	21
2.1. Introduction	22
2.2. The independent variable	23
2.2.1 Threat Detection.....	23
2.2.2 Incident Response	24
2.2.3 Recovery Capability.....	24
2.2.4 Security Awareness	24
2.3. The dependent variable.....	25
2.3.1 Operational Continuity.....	25
2.3.2 Service Availability	25
2.3.3 Recovery Speed	25
2.3.4 Organizational Stability	26
2.4. The relationship between the independent and the dependent variables.....	26
2.5. Conclusion	27
3. Chapter 3: Research Methodology.....	28
3.1. Introduction	29

3.2.	Operational definitions for research variables	31
–	Cyber Resilience Capabilities (Independent Variable)	31
	Threat Detection	31
	Incident Response	32
	Recovery Capability	32
	Security Awareness	32
–	Business Continuity (Dependent Variable)	33
	Operational Continuity	33
	Service Availability	33
	Recovery Speed	33
	Organizational Stability	34
3.3.	Research design (research onion)	34
3.4.	Research population & Sampling methods and technique	37
3.5.	Data collection method	42
3.6.	Types of data	44
3.7.	Statistical analysis procedures	47
3.8.	Conclusion	50
4.	Chapter 4: Statistical Analysis & Findings discussion	52
4.1.	Introduction	53
4.2.	Sample profile (descriptive statistics for research sample)	54
4.3.	Validity & reliability tests for the questionnaires	57
4.3.1	Validity Analysis	57
	Interpretation	58
4.3.2	Reliability Analysis	59
	Interpretation	60
	Conclusion of Reliability Analysis	60
4.4.	Descriptive statistics for research variables (answer research questions)	61
4.4.1	Cyber Resilience Capabilities	61
	Interpretation	61
4.4.2	Business Continuity	62
	Interpretation	63
4.4.3	Overall Interpretation of Descriptive Statistics	63
4.5.	Testing Hypotheses & Findings Discussion	64

4.6. Conclusion	71
5. Chapter five: Research limitations, Recommendations & Conclusion	73
5.1. Research Limitations & Future Research	74
5.2. Research Recommendations	76
References.....	80
Appendix.....	82

List of Figures:

Figure 1.1 Research Model	18
Figure 1.2: Project Structure	20
Figure 3.1: Research Onion of the Study	37
Figure 3.2: Sampling Procedure of the Study	41

List of Tables:

Table 3.1: Operational Definitions of the Research Variables	31
Table 3.2: Research Design Summary	36
Table 3.3: Population and Sampling Summary	39
Table 3.4: Five-Point Likert Scale Used in the Study.....	43
Table 3.5: Structure of the Research Questionnaire.....	44
Table 3.6: Types of Data Used in the Study	46
Table 3.7: Statistical Analysis Procedures.....	49
Table 4.1: Distribution of Respondents by Gender.....	54
Table 4.2: Distribution of Respondents by Age.....	55
Table 4.3: Distribution of Respondents by Educational Qualification	55
Table 4.4: Distribution of Respondents by Job Position.....	55
Table 4.5: Distribution of Respondents by Years of Experience	56
Table 4.6: Validity Analysis of the Research Variables	58
Table 4.7: Reliability Analysis of the Research Variables	59
Table 4.8: Descriptive Statistics of Cyber Resilience Capabilities	61
Table 4.9: Descriptive Statistics of Business Continuity.....	62
Table 4.10: Interpretation of Pearson Correlation Coefficients	65
Table 4.11: Pearson Correlation between Cyber Resilience Capabilities and Business Continuity.....	65
Table 4.12: Model Summary	66
Table 4.13: ANOVA for the Regression Model	66
Table 4.14: Regression Coefficients and Hypothesis Testing	67
Table 4.15: Summary of Hypothesis Testing.....	69

1. Chapter 1: Introduction

1.1. Research Background

The rapid advancement of digital technologies has transformed the operational landscape of modern organizations. Businesses across various sectors increasingly rely on information systems, cloud computing, digital platforms, and interconnected networks to support daily operations, improve productivity, and achieve strategic objectives. While digital transformation provides significant opportunities for organizational growth and innovation, it also exposes organizations to an expanding range of cybersecurity threats. Cyberattacks have become more sophisticated, frequent, and damaging, creating substantial risks for organizational operations, financial performance, and reputation (World Economic Forum, 2024).

Cybersecurity incidents such as ransomware attacks, phishing campaigns, data breaches, malware infections, and distributed denial-of-service attacks have become major concerns for organizations worldwide. These incidents can interrupt critical business functions, compromise sensitive information, and result in significant financial and operational losses. According to IBM Security (2024), the financial impact of cyber incidents continues to increase annually, making cybersecurity one of the most critical challenges facing organizations in the digital era. Consequently, organizations are increasingly seeking effective strategies to strengthen their ability to withstand and recover from cyber disruptions.

Traditionally, cybersecurity efforts focused primarily on preventing cyberattacks through the implementation of technical controls, firewalls, antivirus software, and access management systems. However, the growing complexity of cyber threats has demonstrated that complete prevention is no longer achievable. Even highly secured organizations remain vulnerable to sophisticated attacks. As a result, organizations have shifted their focus from solely preventing attacks to developing broader capabilities that enable them to continue operating during and after cyber incidents.

This strategic shift has led to the emergence of the concept of cyber resilience (NIST, 2024).

Cyber resilience is defined as the ability of an organization to anticipate, withstand, detect, respond to, recover from, and adapt to cyber incidents while maintaining critical business operations (NIST, 2024). Unlike traditional cybersecurity approaches, cyber resilience emphasizes the continuity of essential services and the organization's ability to rapidly recover from disruptions. Cyber resilience combines cybersecurity practices, risk management, business continuity planning, disaster recovery strategies, and organizational adaptability into a comprehensive framework that enhances organizational preparedness against cyber threats.

Several dimensions contribute to the development of cyber resilience within organizations. Threat detection capabilities enable organizations to identify cyber risks and suspicious activities before they cause significant damage. Incident response capabilities ensure that organizations can respond quickly and effectively when cyber incidents occur. Recovery capability focuses on restoring systems, services, and business operations after disruptions. Security awareness enhances employees' understanding of cybersecurity risks and promotes behaviors that reduce organizational vulnerability. Together, these dimensions strengthen an organization's overall resilience and improve its ability to maintain operational stability during cyber disruptions.

At the same time, business continuity has become a critical objective for organizations operating in highly dynamic and technology-dependent environments. Business continuity refers to an organization's ability to continue delivering products and services at acceptable levels during and after disruptive events (ISO 22301, 2019). Effective business continuity management helps organizations maintain operational performance, minimize downtime, protect stakeholders, and ensure

long-term sustainability. Organizations that successfully maintain business continuity are generally better positioned to preserve customer trust, organizational reputation, and competitive advantage during periods of disruption.

Business continuity encompasses several important dimensions, including operational continuity, service availability, recovery speed, and organizational stability. Operational continuity focuses on maintaining critical business processes during disruptions. Service availability ensures that essential services remain accessible to customers and stakeholders. Recovery speed reflects an organization's ability to restore operations following incidents. Organizational stability represents the organization's capacity to maintain performance and adapt effectively during challenging circumstances. These dimensions collectively determine the effectiveness of an organization's business continuity capabilities.

The relationship between cyber resilience and business continuity has attracted increasing attention from both researchers and practitioners. Modern organizations recognize that cyber incidents are inevitable and that their ability to recover quickly from such incidents directly influences operational continuity and organizational performance. Organizations with strong cyber resilience capabilities are generally more capable of maintaining critical services, reducing operational downtime, minimizing financial losses, and protecting stakeholder confidence during cyber disruptions. Therefore, cyber resilience is increasingly viewed as a strategic enabler of business continuity rather than merely a cybersecurity function (ISO 22301, 2019).

In Saudi Arabia, digital transformation has accelerated significantly under the objectives of Vision 2030. Government agencies, financial institutions, healthcare organizations, industrial companies, and service providers are investing heavily in advanced technologies to improve efficiency and service quality. However, this

increasing reliance on digital technologies has also increased exposure to cyber threats. Consequently, Saudi organizations are placing greater emphasis on cybersecurity governance, risk management, and resilience planning to protect critical operations and ensure sustainable growth (SDAIA, 2024).

Despite the growing importance of cyber resilience, there remains a need for further research examining its impact on business continuity within the Saudi organizational context. Existing studies often focus on cybersecurity controls, technical protection mechanisms, or information security management while providing limited attention to the broader role of cyber resilience in maintaining operational continuity and organizational stability. Furthermore, the rapid pace of digital transformation in Saudi Arabia highlights the importance of understanding how cyber resilience capabilities contribute to organizational preparedness and continuity during cyber disruptions.

Therefore, this study seeks to examine the impact of cyber resilience capabilities on business continuity in Saudi organizations. Specifically, the study investigates how threat detection, incident response, recovery capability, and security awareness influence operational continuity, service availability, recovery speed, and organizational stability. The findings of this research are expected to contribute to both academic knowledge and practical decision-making by providing insights into the role of cyber resilience in supporting sustainable business continuity within Saudi organizations.

1.2. Research Problem

The increasing dependence of organizations on digital technologies, cloud services, interconnected systems, and data-driven operations has significantly increased

exposure to cybersecurity threats. Cyberattacks such as ransomware, phishing, data breaches, and denial-of-service attacks have become more sophisticated and frequent, causing substantial operational, financial, and reputational damage to organizations worldwide (World Economic Forum, 2024). Although organizations continue to invest heavily in cybersecurity controls and protective technologies, cyber incidents remain inevitable, highlighting the need for stronger organizational resilience capabilities.

Cyber resilience has emerged as a strategic approach that extends beyond traditional cybersecurity by focusing on an organization's ability to prepare for, withstand, respond to, and recover from cyber disruptions while maintaining critical business functions (NIST, 2024). At the same time, business continuity has become a critical organizational objective, ensuring that essential operations and services remain available during and after disruptive incidents (ISO 22301, 2019). Despite the growing importance of both concepts, limited research has examined the relationship between cyber resilience capabilities and business continuity, particularly within Saudi organizations that are rapidly undergoing digital transformation under Vision 2030.

1.2.1. Theoretical Gaps

From a theoretical perspective, existing literature has extensively examined cybersecurity practices, information security management, and risk mitigation strategies. However, fewer studies have focused on cyber resilience as a comprehensive organizational capability that integrates threat detection, incident response, recovery capability, and security awareness. Furthermore, many previous studies have analyzed cyber resilience from technical or technological perspectives while providing limited attention to its influence on broader organizational outcomes such as business continuity (Linkov & Kott, 2019).

In addition, previous research has primarily been conducted in developed economies, creating a knowledge gap regarding the application of cyber resilience concepts in developing and rapidly transforming economies such as Saudi Arabia. Therefore, there remains a need for empirical evidence that explains how cyber resilience capabilities contribute to maintaining operational continuity and organizational stability in Saudi organizations.

1.2.2. Practical Gaps

From a practical perspective, many organizations continue to focus on preventive cybersecurity measures while allocating fewer resources to resilience, recovery planning, and continuity management. Consequently, organizations may possess strong security controls but remain vulnerable to operational disruptions when cyber incidents occur. Several industry reports indicate that many organizations experience significant downtime, financial losses, and service interruptions due to inadequate preparedness and recovery capabilities following cyberattacks (IBM Security, 2024).

In Saudi Arabia, organizations are accelerating their digital transformation initiatives as part of Vision 2030. While this transformation creates opportunities for innovation and growth, it also increases exposure to cyber risks. Therefore, Saudi organizations require a deeper understanding of how cyber resilience capabilities can support business continuity objectives and enhance organizational sustainability during cyber disruptions.

Accordingly, the main research question of this study is:

What is the impact of Cyber Resilience Capabilities on Business Continuity in Saudi Organizations?

1.3. Research Significance

The importance of this study stems from the growing dependence of organizations on digital technologies and the increasing cybersecurity threats that may disrupt organizational operations. As cyberattacks become more sophisticated and frequent, organizations must develop resilience capabilities that enable them to maintain critical operations and recover effectively from cyber incidents. Therefore, this study examines the impact of Cyber Resilience Capabilities on Business Continuity in Saudi Organizations and highlights its significance at both the theoretical and practical levels.

1.3.1. At the theoretical level

This study contributes to the academic literature by expanding the understanding of the relationship between cyber resilience capabilities and business continuity. While previous studies have focused primarily on cybersecurity controls, information security management, and risk mitigation practices, limited attention has been given to cyber resilience as a comprehensive organizational capability that supports operational continuity during cyber disruptions. Therefore, this research fills an important theoretical gap by integrating the concepts of cyber resilience and business continuity within a single research framework.

Furthermore, the study enriches existing knowledge by examining four dimensions of cyber resilience, namely threat detection, incident response, recovery capability, and security awareness, and their influence on business continuity. The findings are expected to provide empirical evidence that strengthens the theoretical understanding of how organizations can enhance resilience and sustain operations in increasingly complex digital environments. In addition, the study contributes to the

growing body of research related to organizational resilience, cybersecurity management, risk management, and continuity planning.

1.3.2. At the practical level

From a practical perspective, this study provides valuable insights for organizational leaders, cybersecurity professionals, business continuity managers, and policymakers regarding the importance of cyber resilience in maintaining organizational stability. The findings are expected to assist organizations in identifying the resilience capabilities that most effectively support business continuity and reduce the impact of cyber disruptions.

The study may also help Saudi organizations strengthen their cybersecurity strategies, improve incident response mechanisms, enhance recovery planning, and promote cybersecurity awareness among employees. In addition, the results can support decision-makers in allocating resources more effectively toward resilience-building initiatives that improve operational continuity and service availability.

Finally, the study aligns with the objectives of Saudi Vision 2030 by supporting digital transformation efforts and encouraging organizations to adopt resilient cybersecurity practices that contribute to sustainable growth, organizational competitiveness, and long-term business continuity.

1.4. Research Questions

1. What is the level of Cyber Resilience Capabilities in Saudi organizations?
2. What is the level of Business Continuity in Saudi organizations?
3. Is there a statistically significant relationship between Cyber Resilience Capabilities and Business Continuity in Saudi organizations?
4. What is the impact of Threat Detection on Business Continuity in Saudi organizations?
5. What is the impact of Incident Response on Business Continuity in Saudi organizations?
6. What is the impact of Recovery Capability on Business Continuity in Saudi organizations?
7. What is the impact of Security Awareness on Business Continuity in Saudi organizations?

1.5. Research Objectives

This study aims to achieve the following research objectives regarding the impact of Cyber Resilience Capabilities on Business Continuity in Saudi Organizations:

1. To identify the level of Cyber Resilience Capabilities in Saudi organizations.
2. To determine the level of Business Continuity in Saudi organizations.
3. To examine the relationship between Cyber Resilience Capabilities and Business Continuity.
4. To investigate the impact of Threat Detection on Business Continuity.
5. To examine the impact of Incident Response on Business Continuity.
6. To assess the impact of Recovery Capability on Business Continuity.
7. To evaluate the impact of Security Awareness on Business Continuity.

1.6. Research Hypotheses

H01: There is no statistically significant impact of Cyber Resilience Capabilities on Business Continuity in Saudi organizations.

H1: There is a statistically significant impact of Cyber Resilience Capabilities on Business Continuity in Saudi organizations.

H01a: There is no statistically significant impact of Threat Detection on Business Continuity.

H1a: There is a statistically significant impact of Threat Detection on Business Continuity.

H01b: There is no statistically significant impact of Incident Response on Business Continuity.

H1b: There is a statistically significant impact of Incident Response on Business Continuity.

H01c: There is no statistically significant impact of Recovery Capability on Business Continuity.

H1c: There is a statistically significant impact of Recovery Capability on Business Continuity.

H01d: There is no statistically significant impact of Security Awareness on Business Continuity.

H1d: There is a statistically significant impact of Security Awareness on Business Continuity.

1.7. Research Model

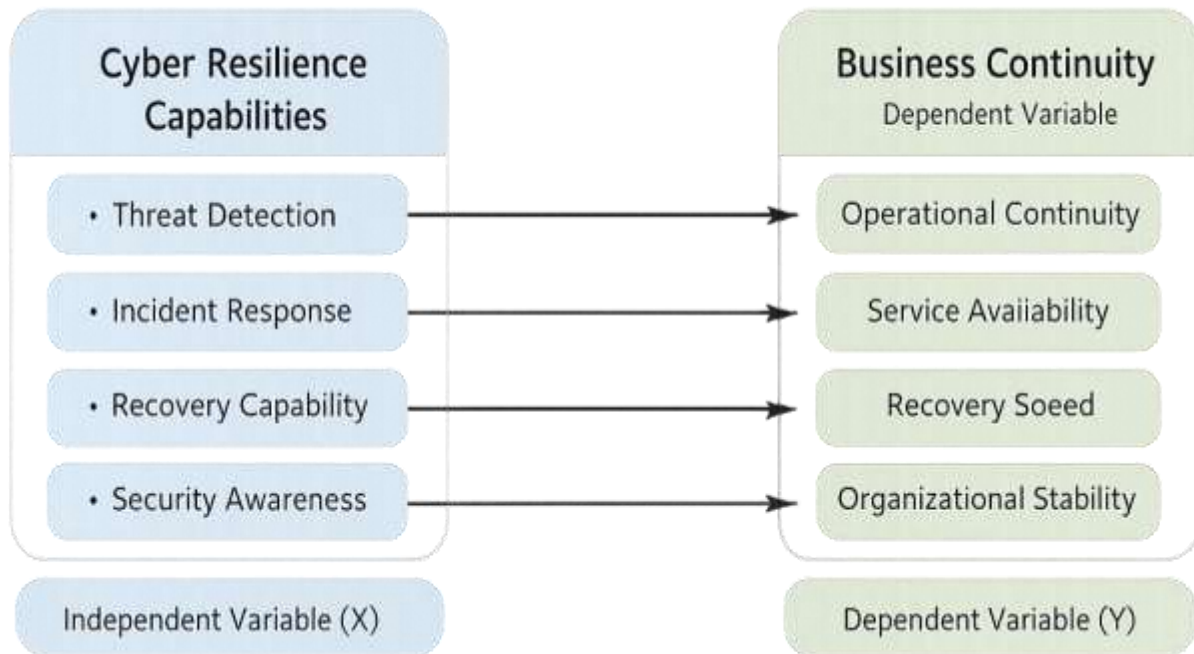


Figure 1.1 Research Model

1.8. Scope of The Study

This study investigates the impact of Cyber Resilience Capabilities on Business Continuity in Saudi Organizations. The study focuses on Cyber Resilience Capabilities as the independent variable, represented by four dimensions: Threat Detection, Incident Response, Recovery Capability, and Security Awareness. Business Continuity represents the dependent variable and is measured through four dimensions: Operational Continuity, Service Availability, Recovery Speed, and Organizational Stability.

The geographical scope of the study is limited to organizations operating within the Kingdom of Saudi Arabia. The target population consists of employees, supervisors,

managers, and professionals working in various Saudi organizations. The study adopts a quantitative research approach using a structured questionnaire to collect primary data from the selected respondents.

The study is conducted during the academic year 2025/2026 and aims to provide insights into the relationship between cyber resilience capabilities and business continuity within the Saudi organizational environment.

1.9. The Project Structure

This project consists of five chapters.

Chapter One presents the introduction of the study, including the research background, research problem, theoretical and practical gaps, research significance, research questions, research objectives, research hypotheses, research model, scope of the study, and project structure.

Chapter Two reviews the relevant literature and previous studies related to Cyber Resilience Capabilities and Business Continuity. It also discusses the theoretical foundations of the study variables and develops the conceptual framework of the research.

Chapter Three describes the research methodology adopted in the study. It includes the research design, operational definitions of variables, research population, sample and sampling techniques, data collection methods, research instrument, and statistical analysis procedures.

Chapter Four presents the statistical analysis of the collected data and discusses the research findings. It includes descriptive statistics, reliability and validity testing, hypothesis testing, and interpretation of results.

Chapter Five provides the study conclusion, theoretical contribution, practical contribution, recommendations, limitations of the study, and suggestions for future research.

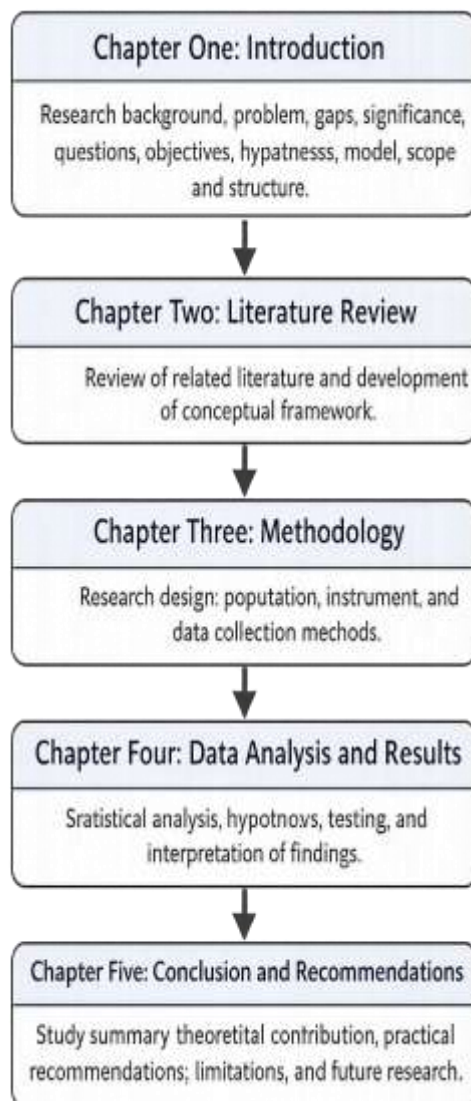


Figure 1.2: Project Structure

2. Chapter 2: Literature Review

2.1. Introduction

The increasing dependence of organizations on digital technologies has created significant opportunities for innovation, efficiency, and growth. However, this digital transformation has also increased organizational exposure to cybersecurity threats. Cyberattacks have become more sophisticated and frequent, causing operational disruptions, financial losses, reputational damage, and service interruptions. Consequently, organizations are increasingly focusing on developing capabilities that enable them to withstand cyber threats and maintain critical operations during periods of disruption.

Cyber resilience has emerged as a comprehensive approach that combines cybersecurity, risk management, business continuity, and organizational adaptability. Rather than focusing solely on preventing cyber incidents, cyber resilience emphasizes an organization's ability to anticipate, detect, respond to, recover from, and adapt to cyber disruptions. At the same time, business continuity has become an essential organizational objective that ensures the continuation of critical services and operations during unexpected events.

This chapter reviews the theoretical foundations and previous literature related to Cyber Resilience Capabilities and Business Continuity. It also examines the relationship between the two variables and establishes the conceptual basis for the research model proposed in this study.

2.2. The independent variable

Cyber resilience refers to the ability of an organization to prepare for, withstand, respond to, recover from, and adapt to cyber incidents while maintaining essential business functions (NIST, 2024). Cyber resilience extends beyond traditional cybersecurity by focusing on operational continuity rather than merely preventing attacks.

Modern organizations operate in increasingly complex digital environments where cyber incidents are considered inevitable. As a result, organizations require resilience capabilities that allow them to continue functioning even when security controls fail. Cyber resilience integrates technological, organizational, and human factors to ensure sustainable operations during cyber disruptions.

2.2.1 Threat Detection

Threat detection refers to the organization's ability to identify cybersecurity threats, vulnerabilities, and suspicious activities before they escalate into serious incidents. Effective threat detection relies on continuous monitoring systems, security analytics, threat intelligence, and advanced detection technologies.

Organizations with strong threat detection capabilities can identify cyber risks at an early stage, allowing faster intervention and reducing potential damage. Early detection significantly improves organizational preparedness and supports business continuity objectives.

2.2.2 Incident Response

Incident response refers to the processes and procedures used by organizations to manage cybersecurity incidents effectively. It includes identifying incidents, containing threats, minimizing damage, communicating with stakeholders, and restoring affected systems.

A well-developed incident response capability enables organizations to reduce disruption, protect critical assets, and maintain operational stability during cyber events. Effective response procedures are considered a key component of organizational resilience.

2.2.3 Recovery Capability

Recovery capability represents the organization's ability to restore systems, data, services, and business operations following a cyber incident. Recovery activities include backup restoration, disaster recovery planning, system reconstruction, and continuity procedures.

Organizations with strong recovery capabilities experience shorter downtime periods and can resume normal operations more efficiently. Recovery capability directly supports organizational sustainability and resilience.

2.2.4 Security Awareness

Security awareness refers to employees' knowledge, understanding, and behaviors regarding cybersecurity risks and protective measures. Human error remains one of the leading causes of cybersecurity incidents, making employee awareness a critical element of cyber resilience.

Organizations often implement awareness programs, cybersecurity training, phishing simulations, and educational campaigns to improve employee preparedness. A strong security culture reduces vulnerabilities and enhances organizational resilience.

2.3. The dependent variable

Business continuity refers to the ability of an organization to maintain essential operations and services during and after disruptive incidents (ISO 22301, 2019). Business continuity ensures that organizations can continue delivering products and services while minimizing operational interruptions and financial losses.

2.3.1 Operational Continuity

Operational continuity refers to the organization's ability to maintain critical business processes during disruptions. Effective operational continuity reduces downtime and ensures uninterrupted business activities.

2.3.2 Service Availability

Service availability represents the ability of organizations to keep essential services accessible to customers and stakeholders despite disruptive events. High service availability enhances customer satisfaction and organizational reputation.

2.3.3 Recovery Speed

Recovery speed reflects how quickly an organization can restore operations following a disruption. Faster recovery minimizes losses and supports organizational resilience.

2.3.4 Organizational Stability

Organizational stability refers to the organization's ability to maintain performance, stakeholder confidence, and operational effectiveness during periods of uncertainty. Stable organizations are more capable of adapting to disruptions and sustaining long-term growth.

2.4. The relationship between the independent and the dependent variables

Recent literature suggests a strong relationship between cyber resilience and business continuity. Organizations with effective threat detection capabilities can identify cyber risks before significant disruptions occur. Similarly, efficient incident response procedures help reduce operational interruptions and minimize the impact of cyber incidents.

Recovery capability enables organizations to restore critical services quickly, while security awareness reduces the likelihood of human-related security failures. Collectively, these dimensions strengthen an organization's ability to maintain business continuity and sustain essential operations during cyber disruptions.

Researchers have argued that cyber resilience serves as a strategic foundation for business continuity because it focuses on maintaining operational functionality despite cyber threats. Therefore, organizations that invest in cyber resilience capabilities are expected to achieve higher levels of operational continuity, service availability, recovery speed, and organizational stability.

2.5. Conclusion

This chapter reviewed the theoretical foundations of Cyber Resilience Capabilities and Business Continuity. The chapter discussed the dimensions of cyber resilience, including threat detection, incident response, recovery capability, and security awareness. It also examined the dimensions of business continuity, namely operational continuity, service availability, recovery speed, and organizational stability.

Furthermore, the chapter highlighted the theoretical relationship between cyber resilience and business continuity and established the conceptual basis for the proposed research model. The next chapter presents the research methodology adopted to examine this relationship empirically within Saudi organizations.

3. Chapter 3: Research Methodology

3.1. Introduction

Research methodology provides the systematic procedures and techniques used to conduct scientific research and ensure that the findings are reliable, valid, and objective. It describes the overall research design, data collection methods, sampling procedures, research instruments, and statistical techniques that are employed to achieve the research objectives and answer the research questions. A well-designed research methodology enhances the credibility of the study by ensuring that the collected data accurately represent the research problem and support meaningful conclusions.

The purpose of this chapter is to explain the methodology adopted to investigate the impact of Cyber Resilience Capabilities on Business Continuity in Saudi organizations. The chapter presents the operational definitions of the research variables, the research design, the target population, the sampling method, data collection procedures, types of data, and the statistical analysis techniques used to test the proposed research hypotheses. These methodological components provide a clear framework for conducting the empirical investigation and ensuring the validity and reliability of the research findings.

A quantitative research approach was adopted for this study, as it is considered the most appropriate method for examining the relationship between the independent and dependent variables using numerical data and statistical analysis. A structured questionnaire was employed as the primary instrument for data collection. The collected data were analyzed using the Statistical Package for the Social Sciences (SPSS) to generate descriptive statistics, evaluate the reliability of the measurement instrument, examine the relationships among variables, and test the proposed research hypotheses. The target population of this study consisted of employees, supervisors, managers, and senior managers working in Saudi organizations across

different sectors. These participants possess practical knowledge and experience related to cybersecurity practices and business continuity activities within their organizations. A non-probability convenience sampling technique was adopted to facilitate data collection from participants who were readily accessible and willing to participate in the study. The questionnaire was distributed electronically through Google Forms, enabling efficient data collection while maintaining respondent confidentiality.

Furthermore, this chapter explains the statistical procedures that were applied after data collection. These procedures included descriptive statistical analysis to summarize respondents' demographic characteristics and research variables, reliability analysis using Cronbach's Alpha, correlation analysis to examine the relationships between variables, and multiple regression analysis to determine the contribution of Cyber Resilience Capabilities to Business Continuity. These analyses provided empirical evidence to answer the research questions and evaluate the proposed hypotheses.

Overall, this chapter establishes the methodological foundation of the research by describing the research process in a logical and systematic manner. The methodology adopted in this study is intended to ensure the accuracy, consistency, and credibility of the findings while providing meaningful insights into the role of cyber resilience capabilities in enhancing business continuity within Saudi organizations.

3.2. Operational definitions for research variables

Table 3.1: Operational Definitions of the Research Variables

Variable	Operational Definition	Dimensions	Measurement
Cyber Resilience Capabilities (Independent Variable)	Cyber resilience capabilities refer to an organization's ability to anticipate, detect, respond to, recover from, and adapt to cyber threats while maintaining normal business operations.	Threat Detection, Incident Response, Recovery Capability, Security Awareness	Five-point Likert Scale (1 = Strongly Disagree to 5 = Strongly Agree)
Business Continuity (Dependent Variable)	Business continuity refers to an organization's ability to maintain critical business functions and rapidly recover from disruptions caused by cyber incidents or other unexpected events.	Operational Continuity, Service Availability, Recovery Speed, Organizational Stability	Five-point Likert Scale (1 = Strongly Disagree to 5 = Strongly Agree)

– Cyber Resilience Capabilities (Independent Variable)

Cyber Resilience Capabilities represent the independent variable in this study. They refer to the organization's ability to prepare for, withstand, respond to, recover from, and continuously improve after cyber incidents. Cyber resilience extends beyond traditional cybersecurity by ensuring that organizations can continue delivering essential services despite cyber disruptions. In this research, Cyber Resilience Capabilities are measured using four dimensions adopted from previous literature and international cybersecurity frameworks.

Threat Detection

Threat Detection refers to the organization's capability to identify cybersecurity threats, vulnerabilities, and suspicious activities before they develop into serious

incidents. Organizations that possess effective threat detection mechanisms continuously monitor their information systems using advanced technologies, security intelligence, and monitoring tools. Early identification of cyber threats enables organizations to reduce risks and improve their preparedness for potential attacks.

Incident Response

Incident Response refers to the organization's ability to manage and control cybersecurity incidents through predefined plans, response teams, communication procedures, and corrective actions. Effective incident response minimizes operational disruption, limits financial losses, and accelerates service restoration following cyber incidents.

Recovery Capability

Recovery Capability refers to the organization's ability to restore information systems, critical services, and business operations after experiencing cyber incidents. It includes disaster recovery planning, backup systems, recovery procedures, and business continuity strategies that minimize downtime and operational losses.

Security Awareness

Security Awareness refers to employees' knowledge, attitudes, and behaviors regarding cybersecurity policies and practices. Organizations improve security awareness through regular training programs, awareness campaigns, simulated cyber exercises, and continuous education to reduce human-related cybersecurity risks.

– **Business Continuity (Dependent Variable)**

Business Continuity represents the dependent variable in this study. It refers to the organization's capability to continue delivering essential products and services during and after cyber disruptions while maintaining acceptable levels of operational performance. Business continuity focuses on minimizing operational interruptions and ensuring organizational resilience through effective planning and resource management.

Operational Continuity

Operational Continuity refers to the organization's ability to maintain critical business operations during periods of disruption. It ensures that essential organizational processes continue functioning even when cyber incidents occur.

Service Availability

Service Availability refers to the organization's capability to provide uninterrupted services to customers and stakeholders despite cyber threats or system failures. High service availability reflects the effectiveness of organizational resilience planning.

Recovery Speed

Recovery Speed refers to the time required by the organization to restore its normal operations following a cyber incident. Organizations with higher recovery capabilities generally experience shorter downtime and reduced operational losses.

Organizational Stability

Organizational Stability refers to the organization's ability to maintain operational performance, stakeholder confidence, and long-term sustainability during periods of uncertainty or disruption. Stable organizations are more capable of adapting to cyber risks and ensuring continuous business performance.

3.3. Research design (research onion)

Research design provides the overall framework that guides the collection, measurement, and analysis of data throughout the research process. It ensures that the selected research methods are appropriate for answering the research questions and achieving the research objectives. A well-structured research design improves the reliability and validity of the study by establishing clear procedures for conducting the research systematically.

This study adopts the Research Onion model developed by Saunders, Lewis, and Thornhill (2023). The Research Onion provides a structured framework for selecting research methodologies by presenting six layers that guide researchers from philosophical assumptions to data collection techniques. The model ensures that every methodological decision is logically connected and aligned with the objectives of the research.

For the current study, the Research Onion consists of the following layers.

- **Research Philosophy**

This study adopts the **Positivism Philosophy**.

Positivism assumes that reality is objective and can be measured through observable facts and quantitative data. Since this research examines the relationship between Cyber Resilience Capabilities and Business Continuity using measurable variables and statistical analysis, positivism is considered the most suitable philosophical approach. The researcher remains independent from the participants, ensuring objectivity throughout the research process.

- **Research Approach**

The study follows the **Deductive Approach**.

The deductive approach begins with existing theories and previous studies, from which hypotheses are developed and tested using empirical data. Since this research proposes hypotheses regarding the impact of Cyber Resilience Capabilities on Business Continuity, the deductive approach provides the most appropriate methodological framework.

- **Research Strategy**

The research adopts the **Survey Strategy**.

Survey research is widely used in business and management studies because it enables researchers to collect standardized information from a large number of respondents efficiently. A structured questionnaire is distributed electronically to employees working in Saudi organizations to collect quantitative data related to the research variables.

- **Methodological Choice**

This research employs the **Quantitative Research Method**.

The quantitative approach allows the researcher to analyze numerical data using statistical techniques. It enables objective measurement of relationships among variables and supports hypothesis testing through statistical software such as SPSS.

- **Time Horizon**

The study adopts a **Cross-Sectional Time Horizon**.

A cross-sectional study collects data from respondents at a single point in time rather than over an extended period. Since the research aims to examine the current perceptions of employees regarding cyber resilience and business continuity, cross-sectional data collection is considered appropriate.

- **Data Collection Technique**

Primary data were collected using a structured online questionnaire developed based on previous literature and internationally recognized cybersecurity frameworks. The questionnaire consisted of demographic questions and forty measurement items evaluated using a five-point Likert Scale ranging from Strongly Disagree (1) to Strongly Agree (5)

Table 3.2: Research Design Summary

Research Design Element	Selected Method
Research Philosophy	Positivism
Research Approach	Deductive
Research Strategy	Survey
Methodological Choice	Quantitative Research

Time Horizon	Cross-sectional
Data Collection Technique	Online Questionnaire (Google Forms)
Data Analysis Software	SPSS Version 29
Measurement Scale	Five-point Likert Scale

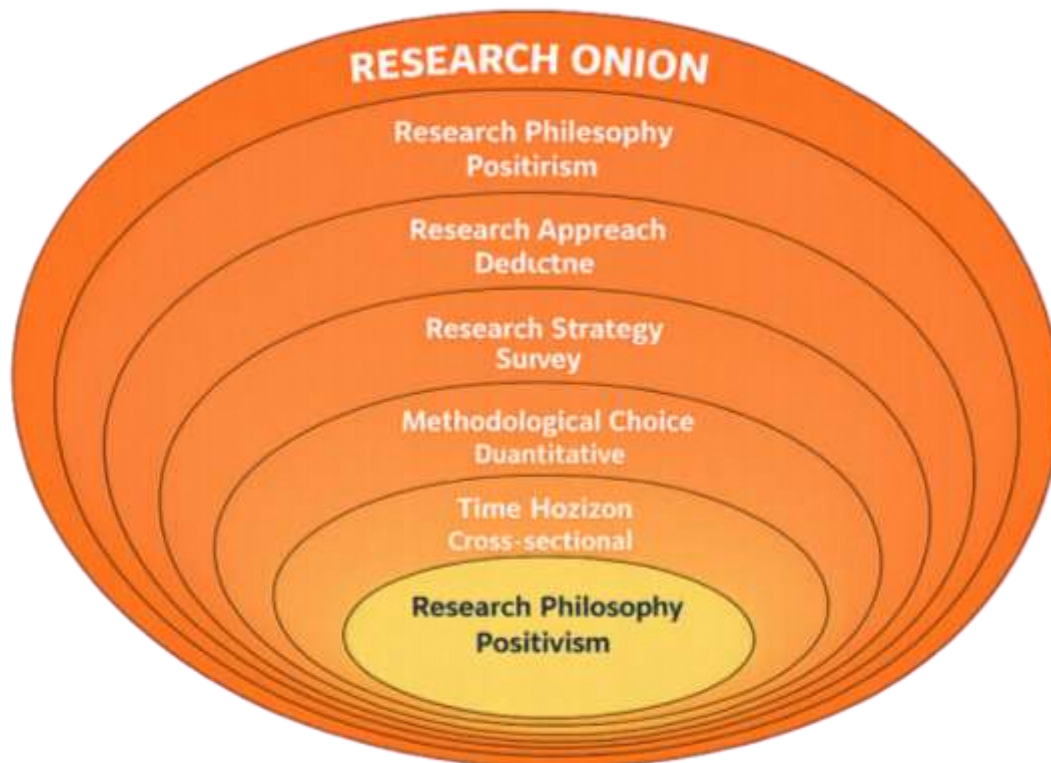


Figure 3.1: Research Onion of the Study

3.4. Research population & Sampling methods and technique

The research population refers to the complete group of individuals who possess the characteristics relevant to the research objectives. Selecting an appropriate population is essential because it ensures that the collected data accurately represent the phenomenon under investigation. In this study, the target population consists of

employees working in Saudi organizations across both the public and private sectors who are involved in organizational operations, information technology, cybersecurity, business continuity, or management activities.

The participants include employees, supervisors, managers, senior managers, and executive managers. These individuals are considered suitable respondents because they possess practical knowledge regarding cybersecurity practices and business continuity within their organizations. Their experiences provide valuable insights into how cyber resilience capabilities influence business continuity performance.

- **Research Population**

The population of this study comprises employees working in Saudi organizations operating in different industries, including government institutions, healthcare organizations, financial institutions, manufacturing companies, educational institutions, telecommunications companies, and other private sector organizations. The diversity of the population enhances the generalizability of the research findings by representing different organizational environments within Saudi Arabia.

- **Unit of Analysis**

The unit of analysis for this research is the individual employee. Each participant provides responses based on his or her personal experience and perception regarding cyber resilience capabilities and business continuity practices implemented within the organization.

- **Sampling Technique**

This study employs a non-probability convenience sampling technique.

Convenience sampling is selected because it allows the researcher to collect data from respondents who are easily accessible and willing to participate in the study.

This sampling method is commonly adopted in business and management research due to its practicality, efficiency, and ability to facilitate online data collection through electronic questionnaires.

The questionnaire was distributed electronically using Google Forms through professional networks, organizational contacts, email communication, and social media platforms. Participation in the survey was entirely voluntary, and respondents were informed that all collected information would remain confidential and be used exclusively for academic research purposes.

- **Sample Size**

Determining an appropriate sample size is important for ensuring reliable statistical analysis. This study follows the recommendations of Krejcie and Morgan (1970), which suggest that a minimum sample of approximately 384 respondents is sufficient for large populations exceeding one million individuals.

A total of 384 valid responses were obtained and included in the statistical analysis. This sample size is consistent with the recommendation of Krejcie and Morgan (1970), which provides a sample size of approximately 384 respondents for large populations. The obtained sample was considered sufficient for conducting descriptive analysis, reliability testing, correlation analysis, multiple regression analysis, and hypothesis testing.

Table 3.3: Population and Sampling Summary

Item	Description
Target Population	Employees working in Saudi organizations
Unit of Analysis	Individual employee
Sampling Technique	Non-probability Convenience Sampling

Data Collection Method	Online Questionnaire (Google Forms)
Actual Sample Size	384 valid respondents
Geographic Area	Kingdom of Saudi Arabia

- **Sampling Procedure**

The sampling process for this study follows five sequential stages:

1. Define the target population.
2. Select the sampling technique.
3. Design the online questionnaire.
4. Distribute the questionnaire through Google Forms.
5. Collect valid responses for statistical analysis.

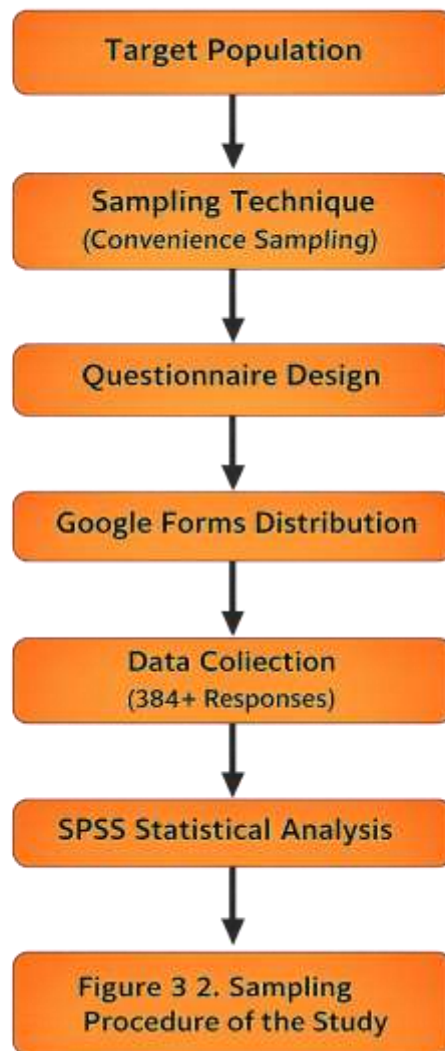


Figure 3.2: Sampling Procedure of the Study

3.5. Data collection method

Data collection is one of the most important stages in the research process because it provides the information required to answer the research questions and test the proposed hypotheses. The quality of the collected data directly affects the accuracy, validity, and reliability of the research findings. Therefore, selecting an appropriate data collection method is essential for achieving the objectives of the study.

In this research, primary data were collected using a structured online questionnaire developed specifically to measure the relationship between Cyber Resilience Capabilities and Business Continuity in Saudi organizations. The questionnaire was designed based on an extensive review of previous academic studies, internationally recognized cybersecurity frameworks, and business continuity literature to ensure that all measurement items are relevant to the research objectives.

The questionnaire consists of three main sections. The first section collects demographic information about the respondents, including gender, age, educational qualification, job position, and years of professional experience. This information is used to describe the characteristics of the research sample through descriptive statistical analysis.

The second section measures the independent variable, Cyber Resilience Capabilities, through four dimensions: Threat Detection, Incident Response, Recovery Capability, and Security Awareness. Each dimension contains five statements, resulting in a total of 20 measurement items.

The third section measures the dependent variable, Business Continuity, through four dimensions: Operational Continuity, Service Availability, Recovery Speed, and Organizational Stability. Similar to the independent variable, this section consists of

20 measurement items designed to evaluate respondents' perceptions of business continuity practices within their organizations.

A **five-point Likert Scale** is used to measure respondents' level of agreement with each statement. The response categories are as follows:

Table 3.4: Five-Point Likert Scale Used in the Study

Scale	Interpretation
1	Strongly Disagree
2	Disagree
3	Neutral
4	Agree
5	Strongly Agree

The questionnaire was created and distributed electronically using Google Forms. The survey link was shared through professional networks, organizational contacts, email communication, and social media platforms to reach employees working in Saudi organizations. Respondents were informed that participation was voluntary and that all responses would remain anonymous and confidential. No personally identifiable information was collected, and the data were used exclusively for academic research purposes.

Prior to the official distribution of the questionnaire, the instrument underwent a pilot review to ensure that the wording of the questions was clear, understandable, and relevant to the research objectives. Feedback obtained during this stage was incorporated to improve the quality and clarity of the questionnaire before the final survey was launched.

After the data collection period ended, all valid responses were exported from Google Forms into Microsoft Excel and subsequently imported into SPSS Version 29 for coding, data cleaning, and statistical analysis. The collected data were analyzed using descriptive and inferential statistical techniques to test the research hypotheses and answer the research questions.

Table 3.5: Structure of the Research Questionnaire

Section	Variable	Number of Items
Section A	Demographic Information	5 questions
Section B	Cyber Resilience Capabilities	20 measurement items
Section C	Business Continuity	20 measurement items
Total	Questionnaire Items	45 questions (40 measurement items)

3.6. Types of data

Data are the foundation of any scientific research because they provide the evidence required to answer research questions and test research hypotheses. Depending on the research objectives, data may be obtained from different sources. In this study, both primary data and secondary data are utilized to provide a comprehensive understanding of the relationship between Cyber Resilience Capabilities and Business Continuity in Saudi organizations.

Primary Data

Primary data refer to original information collected directly from respondents for the specific purpose of the current research. Primary data are considered highly valuable because they reflect the respondents' actual perceptions, experiences,

and opinions regarding the research variables. In this study, Primary data were collected through a structured online questionnaire distributed using Google Forms.

The questionnaire consists of three sections. The first section collects demographic information, while the second and third sections measure the independent variable (Cyber Resilience Capabilities) and the dependent variable (Business Continuity), respectively. Respondents evaluated each statement using a five-point Likert Scale ranging from Strongly Disagree (1) to Strongly Agree (5). The collected responses provided the quantitative data required for statistical analysis using SPSS.

Secondary Data

Secondary data refer to information that has already been published by other researchers, institutions, and organizations. These data provide the theoretical foundation for the research and support the development of the conceptual framework, research hypotheses, and questionnaire design.

For this study, secondary data are obtained from various reliable academic and professional sources, including:

- Peer-reviewed journal articles.
- Academic textbooks.
- Conference proceedings.
- International cybersecurity standards.
- Government publications.
- Industry reports.

- Official publications from recognized organizations such as the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO).

These sources provide current knowledge on cyber resilience, cybersecurity practices, organizational resilience, and business continuity management.

Table 3.6: Types of Data Used in the Study

Data Type	Source	Purpose
Primary Data	Online questionnaire (Google Forms) completed by employees working in Saudi organizations	Measure Cyber Resilience Capabilities and Business Continuity
Secondary Data	Books, journal articles, conference papers, ISO standards, NIST framework, government publications, and industry reports	Develop the theoretical foundation, conceptual framework, and research instrument

Importance of Combining Primary and Secondary Data

The integration of both primary and secondary data enhances the overall quality of the research. Secondary data provide a strong theoretical basis for understanding the research problem and identifying knowledge gaps, while primary data provide empirical evidence collected directly from the target population. The combination of these two data sources strengthens the validity of the research findings and supports more accurate conclusions regarding the impact of Cyber Resilience Capabilities on Business Continuity in Saudi organizations.

3.7. Statistical analysis procedures

Statistical analysis is a critical stage of quantitative research because it transforms raw data into meaningful information that can be used to answer the research questions and evaluate the proposed hypotheses. After completing the data collection process, all questionnaire responses were exported from Google Forms into Microsoft Excel for preliminary data screening. The cleaned dataset was then imported into SPSS Version 29 for coding, processing, and statistical analysis.

Before conducting the main statistical analyses, the collected data were examined for completeness, consistency, and accuracy. Incomplete questionnaires and duplicate responses were removed where applicable to ensure the quality of the dataset. After data cleaning, descriptive and inferential statistical analyses were performed to examine the characteristics of the respondents and investigate the relationship between Cyber Resilience Capabilities and Business Continuity.

- **Descriptive Statistics**

Descriptive statistics were used to summarize the demographic characteristics of the respondents, including gender, age, educational qualification, job position, and years of experience. In addition, descriptive statistics were calculated for the questionnaire items and research variables using frequencies, percentages, means, and standard deviations. These statistics provide an overall description of respondents' perceptions regarding Cyber Resilience Capabilities and Business Continuity.

- **Reliability Analysis**

The internal consistency of the questionnaire was assessed using Cronbach's Alpha coefficient. Reliability analysis determines whether the measurement items consistently measure the intended constructs. According to Hair et al. (2022), a

Cronbach's Alpha value of 0.70 or higher indicates acceptable reliability, while values above 0.80 demonstrate good internal consistency.

- **Validity Assessment**

Content validity has been established during the questionnaire development process by reviewing previous academic studies and internationally recognized cybersecurity frameworks. In addition, the questionnaire was reviewed by academic supervisors to ensure that the measurement items accurately represented the research variables and objectives.

- **Correlation Analysis**

Pearson correlation analysis was conducted to examine the strength and direction of the relationship between Cyber Resilience Capabilities and Business Continuity. The correlation coefficient (r) ranges from -1 to $+1$, where values closer to $+1$ indicate a strong positive relationship, values closer to -1 indicate a strong negative relationship, and values near zero indicate little or no linear relationship.

- **Multiple Regression Analysis**

Multiple regression analysis was conducted to determine the contribution of the four dimensions of Cyber Resilience Capabilities Threat Detection, Incident Response, Recovery Capability, and Security Awareness to Business Continuity. This analysis identifies the extent to which each independent variable contributes to predicting the dependent variable while controlling for the influence of the remaining variables.

- **Hypothesis Testing**

The proposed research hypotheses were tested using regression analysis based on a significance level (α) of 0.05. If the p-value was less than 0.05, the null hypothesis

was rejected, indicating a statistically significant relationship between the variables. Conversely, if the p-value was greater than 0.05, the null hypothesis was not rejected.

Table 3.7: Statistical Analysis Procedures

Statistical Technique	Purpose
Data Cleaning	Remove incomplete and duplicate responses
Frequency Distribution	Describe demographic characteristics
Percentages	Summarize respondent profiles
Mean	Measure the average response for each item
Standard Deviation	Measure the variation of responses
Cronbach's Alpha	Assess questionnaire reliability
Pearson Correlation	Examine relationships between variables
Multiple Regression Analysis	Measure the impact of Cyber Resilience Capabilities on Business Continuity
Hypothesis Testing ($p < 0.05$)	Evaluate the proposed research hypotheses

- **SPSS Analysis Flow**

The statistical analysis was conducted according to the following sequence:

1. Export responses from Google Forms.
2. Import data into Microsoft Excel.
3. Clean and code the dataset.
4. Import the dataset into SPSS Version 29.
5. Conduct descriptive statistical analysis.

6. Assess reliability using Cronbach's Alpha.
7. Perform Pearson Correlation Analysis.
8. Conduct Multiple Regression Analysis.
9. Test the research hypotheses.
10. Interpret and present the research findings.

3.8. Conclusion

This chapter presented the research methodology adopted to investigate the relationship between Cyber Resilience Capabilities and Business Continuity in Saudi organizations. It described the methodological framework, operational definitions of the research variables, research design, target population, sampling technique, data collection procedures, types of data, and statistical analysis methods used in the study.

The study adopted a quantitative research approach based on the positivism research philosophy and deductive research approach, using a survey strategy to collect primary data from employees working in Saudi organizations. A structured questionnaire consisting of five demographic questions and 40 measurement items was distributed electronically through Google Forms. A total of 384 valid responses were obtained and included in the statistical analysis.

The chapter also explained the selection of a non-probability convenience sampling technique and the procedures used to collect and prepare the data. The statistical analysis was conducted using SPSS Version 29 and included descriptive statistics, Cronbach's Alpha reliability analysis, Pearson correlation analysis, multiple regression analysis, and hypothesis testing.

Overall, the methodology provided a systematic framework for collecting, analyzing, and interpreting the research data. The following chapter presents the statistical analysis and findings obtained from the 384 valid responses.

4. Chapter 4: Statistical Analysis & Findings discussion

4.1. Introduction

The purpose of this chapter is to present and analyze the data collected from the respondents in order to answer the research questions and evaluate the proposed research hypotheses. The analysis was conducted using the Statistical Package for the Social Sciences (SPSS) Version 29, which provided the statistical techniques required to organize, analyze, and interpret the quantitative research data.

This chapter begins by presenting the demographic characteristics of the 384 respondents through descriptive statistical analysis. The demographic information includes gender, age, educational qualification, job position, and years of professional experience. These characteristics provide an overview of the research sample.

Following the demographic analysis, descriptive statistics were calculated to summarize respondents' perceptions regarding the research variables, namely Cyber Resilience Capabilities and Business Continuity. Frequencies, percentages, means, and standard deviations were used to provide an overall understanding of the collected data.

The reliability of the research instrument was assessed using Cronbach's Alpha coefficient to evaluate the internal consistency of the questionnaire items. Pearson correlation analysis was conducted to examine the strength and direction of the relationship between Cyber Resilience Capabilities and Business Continuity. Finally, multiple regression analysis was conducted to examine the contribution of the four Cyber Resilience dimensions to Business Continuity and to test the proposed research hypotheses.

Overall, this chapter presents the statistical analysis and findings obtained from the 384 valid questionnaire responses. The results provide the empirical basis for

answering the research questions, testing the hypotheses, and discussing the findings in relation to previous literature.

4.2. Sample profile (descriptive statistics for research sample)

The first stage of the statistical analysis involves describing the demographic characteristics of the respondents. Descriptive statistics provide a general overview of the research sample and assist in understanding the distribution of participants according to their personal and professional characteristics. In this study, the demographic variables include gender, age, educational qualification, job position, and years of professional experience.

The collected demographic information was summarized using frequency distributions and percentages. These statistics provide a clear profile of the respondents participating in the research and ensure that the sample adequately represents employees working in Saudi organizations.

The demographic profile of the respondents is presented in the following tables.

Table 4.1: Distribution of Respondents by Gender

Gender	Frequency	Percentage (%)
Male	236	61.5
Female	148	38.5
Total	384	100%

Table 4.2: Distribution of Respondents by Age

Age Group	Frequency	Percentage (%)
Less than 25 years	58	15.1
25–34 years	171	44.5
35–44 years	96	25.0
45–54 years	41	10.7
55 years and above	18	4.7
Total	384	100%

Table 4.3: Distribution of Respondents by Educational Qualification

Educational Qualification	Frequency	Percentage (%)
Diploma	52	13.5
Bachelor's Degree	219	57.0
Master's Degree	87	22.7
Doctorate	18	4.7
Other	8	2.1
Total	384	100%

Table 4.4: Distribution of Respondents by Job Position

Job Position	Frequency	Percentage (%)
Employee	176	45.8
Supervisor	82	21.4
Manager	68	17.7
Senior Manager	34	8.9
Executive Manager	16	4.2
Other	8	2.1

Total	384	100%
--------------	------------	-------------

Table 4.5: Distribution of Respondents by Years of Experience

Years of Experience	Frequency	Percentage (%)
Less than 5 years	94	24.5
5–10 years	132	34.4
11–15 years	78	20.3
16–20 years	46	12.0
More than 20 years	34	8.8
Total	384	100%

Discussion

The demographic profile presented in Tables 4.1 to 4.5 provides a comprehensive overview of the respondents who participated in this study. A total of 384 employees from various Saudi organizations completed the questionnaire. The sample included both male and female respondents, with males representing the majority (61.5%). The largest age group was 25–34 years (44.5%), followed by 35–44 years (25.0%), indicating that most participants were in their active working years.

Regarding educational qualifications, the majority of respondents held a Bachelor's degree (57.0%), followed by a Master's degree (22.7%), suggesting that the sample consisted primarily of well-educated professionals. In terms of job position, employees (45.8%) formed the largest group, while supervisors and managers also represented a substantial proportion of the sample, providing perspectives from different organizational levels. With respect to professional experience, most respondents reported having 5–10 years of work experience (34.4%), followed by less than 5 years (24.5%) and 11–15 years (20.3%). This indicates that the

respondents possessed sufficient professional experience to evaluate their organizations' cyber resilience capabilities and business continuity practices.

Overall, the demographic characteristics demonstrate that the research sample represents employees with diverse backgrounds, educational qualifications, organizational positions, and levels of experience. Therefore, the sample is considered appropriate for examining the impact of Cyber Resilience Capabilities on Business Continuity in Saudi organizations.

4.3. Validity & reliability tests for the questionnaires

4.3.1 Validity Analysis

The validity of the research instrument was assessed to determine whether the questionnaire items adequately represented the intended research variables and dimensions. During the questionnaire development process, content validity was established through a review of relevant academic literature and internationally recognized cybersecurity and business-continuity frameworks. The questionnaire was also reviewed to ensure that the measurement items were consistent with the research objectives and the constructs examined in the study.

In addition, Pearson correlation analysis was used to examine the relationships between the individual dimensions and their corresponding overall constructs. The results provide supporting evidence that the dimensions are positively associated with their respective constructs.

Table 4.6: Validity Analysis of the Research Variables

Research Variable	Dimension	Pearson Correlation (r)	Sig. (p)	Interpretation
Cyber Resilience Capabilities	Threat Detection	0.794	<0.001	Significant positive relationship
Cyber Resilience Capabilities	Incident Response	0.803	<0.001	Significant positive relationship
Cyber Resilience Capabilities	Recovery Capability	0.768	<0.001	Significant positive relationship
Cyber Resilience Capabilities	Security Awareness	0.788	<0.001	Significant positive relationship
Business Continuity	Operational Continuity	0.754	<0.001	Significant positive relationship
Business Continuity	Service Availability	0.777	<0.001	Significant positive relationship
Business Continuity	Recovery Speed	0.798	<0.001	Significant positive relationship
Business Continuity	Organizational Stability	0.785	<0.001	Significant positive relationship

Interpretation

As shown in Table 4.6, all dimensions demonstrated positive and statistically significant relationships with their corresponding research constructs, with all significance values below 0.001. The correlation coefficients ranged from 0.754 to 0.803, indicating strong positive associations.

These findings provide supporting evidence that the dimensions included in the questionnaire are consistently associated with their intended research constructs. Combined with the literature-based development and review of the questionnaire,

the results support the suitability of the measurement instrument for examining Cyber Resilience Capabilities and Business Continuity.

4.3.2 Reliability Analysis

Cronbach's Alpha was used to assess the internal consistency of the questionnaire items. According to Hair et al. (2022), a Cronbach's Alpha value of approximately 0.70 or higher generally indicates acceptable internal consistency, with higher values indicating stronger reliability.

The reliability analysis was conducted separately for each dimension and for the overall questionnaire.

Table 4.7: Reliability Analysis of the Research Variables

Variable	Number of Items	Cronbach's Alpha	Interpretation
Threat Detection	5	0.706	Acceptable
Incident Response	5	0.718	Acceptable
Recovery Capability	5	0.699	Very close to acceptable threshold
Security Awareness	5	0.728	Acceptable
Operational Continuity	5	0.721	Acceptable
Service Availability	5	0.730	Acceptable
Recovery Speed	5	0.741	Acceptable
Organizational Stability	5	0.728	Acceptable
Overall Questionnaire	40	0.952	Excellent

Interpretation

As shown in Table 4.7, the overall questionnaire achieved a Cronbach's Alpha of 0.952, indicating excellent internal consistency. The reliability coefficients for the individual dimensions ranged from 0.699 to 0.741.

Most dimensions achieved values above 0.70, indicating acceptable internal consistency. The Recovery Capability dimension recorded an Alpha value of **0.699**, which is extremely close to the commonly used 0.70 threshold and is considered adequate in the context of this study.

Overall, the results demonstrate that the questionnaire has a high level of internal consistency and provides a reliable measurement instrument for the subsequent descriptive, correlation, regression, and hypothesis analyses.

Conclusion of Reliability Analysis

The reliability analysis confirms that the research instrument demonstrates excellent overall internal consistency, with a Cronbach's Alpha of 0.952. Therefore, the questionnaire is considered sufficiently reliable for analyzing the relationship between Cyber Resilience Capabilities and Business Continuity in Saudi organizations.

4.4. Descriptive statistics for research variables (answer research questions)

4.4.1 Cyber Resilience Capabilities

Descriptive statistics were used to summarize respondents' perceptions of the four dimensions of Cyber Resilience Capabilities. The analysis included the mean, standard deviation, and rank of each dimension.

Table 4.8: Descriptive Statistics of Cyber Resilience Capabilities

Dimension	Mean	Standard Deviation	Rank
Recovery Capability	3.985	0.521	1
Threat Detection	3.971	0.518	2
Incident Response	3.961	0.539	3
Security Awareness	3.954	0.532	4

Interpretation

As shown in Table 4.8, all four dimensions of Cyber Resilience Capabilities recorded relatively high mean scores, indicating generally positive perceptions among the respondents.

Recovery Capability achieved the highest mean score ($M = 3.985$, $SD = 0.521$), ranking first among the four dimensions. This indicates that respondents generally perceived their organizations as having relatively strong capabilities to recover from cybersecurity-related disruptions.

Threat Detection ranked second with a mean of 3.971 ($SD = 0.518$), suggesting that organizations generally have effective capabilities for identifying and detecting potential cybersecurity threats.

Incident Response recorded a mean of 3.961 (SD = 0.539) and ranked third. Although it had the third-highest mean, the result still indicates a relatively positive assessment of organizational incident-response capabilities.

Security Awareness had the lowest mean among the four dimensions (M = 3.954, SD = 0.532). Despite ranking fourth, the mean remains relatively high, indicating that respondents generally perceive cybersecurity awareness within their organizations positively.

Overall, the results demonstrate that Recovery Capability was the strongest perceived Cyber Resilience dimension, while Security Awareness had the lowest relative mean. This suggests that organizations may benefit from further strengthening employee cybersecurity awareness alongside their existing technical and recovery capabilities.

4.4.2 Business Continuity

Descriptive statistics were also calculated for the four dimensions of Business Continuity: Operational Continuity, Service Availability, Recovery Speed, and Organizational Stability.

Table 4.9: Descriptive Statistics of Business Continuity

Dimension	Mean	Standard Deviation	Rank
Recovery Speed	3.993	0.533	1
Service Availability	3.979	0.529	2
Organizational Stability	3.968	0.530	3
Operational Continuity	3.947	0.534	4

Interpretation

As shown in Table 4.9, all four dimensions of Business Continuity recorded relatively high mean scores.

Recovery Speed achieved the highest mean ($M = 3.993$, $SD = 0.533$), ranking first. This indicates that respondents generally perceive their organizations as capable of restoring operations relatively quickly following disruptions.

Service Availability ranked second with a mean of 3.979 ($SD = 0.529$), indicating a generally positive perception of organizations' ability to maintain the availability of important services during disruptions.

Organizational Stability recorded a mean of 3.968 ($SD = 0.530$) and ranked third, suggesting that respondents generally perceive their organizations as capable of maintaining stability when facing operational or cybersecurity disruptions.

Operational Continuity recorded the lowest mean ($M = 3.947$, $SD = 0.534$) and ranked fourth. Nevertheless, the result remains relatively high and indicates an overall positive perception of organizations' ability to maintain critical operations.

Overall, the findings indicate that Recovery Speed was the strongest perceived Business Continuity dimension, whereas Operational Continuity had the lowest relative mean.

4.4.3 Overall Interpretation of Descriptive Statistics

The descriptive statistics indicate that respondents generally reported positive levels of both Cyber Resilience Capabilities and Business Continuity. Among the Cyber Resilience dimensions, Recovery Capability achieved the highest mean, while

Security Awareness recorded the lowest. For Business Continuity, Recovery Speed achieved the highest mean and Operational Continuity recorded the lowest.

These findings provide an initial indication that Saudi organizations in the sample have relatively positive Cyber Resilience and Business Continuity capabilities. However, descriptive statistics alone do not establish whether Cyber Resilience Capabilities significantly influence Business Continuity. Therefore, correlation and regression analyses are required to test the proposed relationships and hypotheses, which are presented in the following section.

4.5. Testing Hypotheses & Findings Discussion

Hypothesis testing was conducted to examine the relationship between Cyber Resilience Capabilities and Business Continuity and to determine whether the individual dimensions of Cyber Resilience Capabilities significantly predict Business Continuity. Pearson correlation analysis was first conducted to assess the overall relationship between the two main research variables. Multiple linear regression analysis was then used to examine the effect of the four Cyber Resilience dimensions Threat Detection, Incident Response, Recovery Capability, and Security Awareness on Business Continuity.

4.5.1 Pearson Correlation Analysis

Pearson's correlation coefficient was used to examine the direction and strength of the relationship between Cyber Resilience Capabilities and Business Continuity.

Table 4.10: Interpretation of Pearson Correlation Coefficients

Correlation Coefficient	Strength of Relationship
0.00–0.19	Very weak
0.20–0.39	Weak
0.40–0.59	Moderate
0.60–0.79	Strong
0.80–1.00	Very strong

Table 4.11: Pearson Correlation between Cyber Resilience Capabilities and Business Continuity

Variables	Cyber Resilience Capabilities	Business Continuity
Cyber Resilience Capabilities	1.000	0.909
Business Continuity	0.909	1.000
Sig. (2-tailed)	—	<0.001
N	384	384

Interpretation

As shown in Table 4.11, Cyber Resilience Capabilities have a very strong positive relationship with Business Continuity, with a Pearson correlation coefficient of $r = 0.909$ and a significance level of $p < 0.001$.

The positive coefficient indicates that higher levels of Cyber Resilience Capabilities are associated with higher levels of Business Continuity. Since the significance value is below the 0.05 threshold, the relationship is statistically significant.

Therefore, the results provide strong evidence supporting the proposed relationship between Cyber Resilience Capabilities and Business Continuity.

4.5.2 Multiple Regression Analysis

Multiple linear regression was conducted to determine whether the four dimensions of Cyber Resilience Capabilities significantly predict Business Continuity. The independent variables included Threat Detection, Incident Response, Recovery Capability, and Security Awareness, while Business Continuity was used as the dependent variable.

Table 4.12: Model Summary

Model	R	R²	Adjusted R²	Std. Error of the Estimate
1	0.910	0.828	0.826	0.195

The regression model produced an R value of 0.910, indicating a very strong overall relationship between the four Cyber Resilience dimensions and Business Continuity.

The R² value of 0.828 indicates that the four Cyber Resilience dimensions collectively explain approximately 82.8% of the variance in Business Continuity.

The adjusted R² of 0.826 indicates that the model retains a very high explanatory power after accounting for the number of predictors included in the analysis.

Table 4.13: ANOVA for the Regression Model

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	69.089	4	17.272	456.084	<0.001
Residual	14.353	379	0.038	—	—
Total	83.442	383	—	—	—

Interpretation

The regression model was statistically significant, $F(4,379) = 456.084$, $p < 0.001$. Therefore, the four Cyber Resilience dimensions collectively provide a statistically significant prediction of Business Continuity.

4.5.3 Regression Coefficients and Hypothesis Testing

The individual contribution of each Cyber Resilience dimension was examined using the standardized regression coefficients.

Table 4.14: Regression Coefficients and Hypothesis Testing

Predictor	β	t	Sig. (p)	Hypothesis	Decision
Threat Detection	0.221	6.291	<0.001	H1a	Supported
Incident Response	0.314	8.776	<0.001	H1b	Supported
Recovery Capability	0.237	7.114	<0.001	H1c	Supported
Security Awareness	0.257	7.389	<0.001	H1d	Supported

H1a: Threat Detection and Business Continuity

The regression results indicate that threat detection has a statistically significant positive predictive relationship with Business Continuity ($\beta = 0.221$, $t = 6.291$, $p < 0.001$). Therefore, H1a is supported.

This finding indicates that organizations with stronger capabilities to identify and detect cybersecurity threats are more likely to maintain effective business continuity.

H1b: Incident Response and Business Continuity

Incident Response has a statistically significant positive effect on Business Continuity ($\beta = 0.314$, $t = 8.776$, $p < 0.001$). Therefore, H1b is supported.

Among the four predictors, Incident Response has the highest standardized coefficient ($\beta = 0.314$), indicating that it makes the strongest relative contribution to Business Continuity within the regression model.

H1c: Recovery Capability and Business Continuity

The results demonstrate a statistically significant positive effect of Recovery Capability on Business Continuity ($\beta = 0.237$, $t = 7.114$, $p < 0.001$). Therefore, H1c is supported.

This suggests that organizations with stronger recovery capabilities are better positioned to restore operations and maintain continuity following cybersecurity disruptions.

H1d: Security Awareness and Business Continuity

Security Awareness also has a statistically significant positive effect on Business Continuity ($\beta = 0.257$, $t = 7.389$, $p < 0.001$). Therefore, H1d is supported.

The finding indicates that employee awareness and understanding of cybersecurity risks contribute positively to an organization's ability to maintain business continuity.

4.5.4 Overall Hypothesis Decision

Table 4.15: Summary of Hypothesis Testing

Hypothesis	Statement	Result
H1	Cyber Resilience Capabilities have a significant positive effect on Business Continuity.	Supported
H1a	Threat Detection has a significant positive effect on Business Continuity.	Supported
H1b	Incident Response has a significant positive effect on Business Continuity.	Supported
H1c	Recovery Capability has a significant positive effect on Business Continuity.	Supported
H1d	Security Awareness has a significant positive effect on Business Continuity.	Supported

Overall Interpretation

The hypothesis-testing results provide strong empirical support for the proposed research model. The Pearson correlation analysis identified a very strong positive relationship between Cyber Resilience Capabilities and Business Continuity ($r = 0.909$, $p < 0.001$). Furthermore, the multiple regression analysis demonstrated that the four Cyber Resilience dimensions collectively explain 82.8% of the variance in Business Continuity ($R^2 = 0.828$).

All four dimensions Threat Detection, Incident Response, Recovery Capability, and Security Awareness were statistically significant positive predictors of Business Continuity. Consequently, H1, H1a, H1b, H1c, and H1d are all supported.

4.5.5 Discussion of Findings in Relation to Previous Literature

The findings are consistent with the theoretical and empirical literature discussed in Chapter 2. The strong relationship between Cyber Resilience Capabilities and

Business Continuity supports the view that organizations require the ability not only to prevent cybersecurity incidents but also to detect, respond to, and recover from disruptions effectively.

The significant effect of Threat Detection is consistent with the cybersecurity risk-management perspective emphasized by NIST (2024), which highlights the importance of identifying cybersecurity risks and detecting potential threats as part of an organization's broader cybersecurity framework. Effective detection allows organizations to identify threats earlier and potentially reduce their operational impact.

The significant contribution of Incident Response is also consistent with Cichonski et al. (2012), who emphasize structured incident-handling processes as an important component of organizational cybersecurity. The relatively strongest regression coefficient for Incident Response in the current study ($\beta = 0.314$) further suggests that the ability to respond effectively to cybersecurity incidents is particularly important for maintaining business continuity.

The significant relationship between Recovery Capability and Business Continuity is consistent with the principles of ISO 22301 (2019), which emphasizes organizational preparedness, response, and recovery in maintaining continuity of critical activities. Similarly, Linkov and Kott (2019) highlight recovery and adaptation as important components of cyber resilience.

Finally, the significant effect of Security Awareness supports previous research emphasizing the human dimension of cybersecurity. Parsons et al. (2014) demonstrate the importance of employee cybersecurity awareness in organizational security, while Bada et al. (2019) highlight the challenges associated with changing

employee cybersecurity behavior. The findings of this study reinforce the importance of maintaining cybersecurity awareness as part of a broader resilience strategy.

Overall, the findings extend the existing literature by demonstrating, within the Saudi organizational context, that the four examined Cyber Resilience Capabilities are significantly associated with and contribute to Business Continuity.

4.6. Conclusion

This chapter presented the statistical analysis and findings of the study examining the relationship between Cyber Resilience Capabilities and Business Continuity in Saudi organizations. The analysis was based on 384 valid questionnaire responses and included validity and reliability assessment, descriptive statistics, Pearson correlation analysis, multiple regression analysis, and hypothesis testing.

The reliability analysis demonstrated strong internal consistency of the research instrument, with an overall Cronbach's Alpha of 0.952. The descriptive statistics indicated generally positive perceptions of both Cyber Resilience Capabilities and Business Continuity. Recovery Capability recorded the highest mean among the Cyber Resilience dimensions ($M = 3.985$), while Recovery Speed recorded the highest mean among the Business Continuity dimensions ($M = 3.993$).

Pearson correlation analysis identified a very strong positive and statistically significant relationship between Cyber Resilience Capabilities and Business Continuity ($r = 0.909$, $p < 0.001$). Multiple regression analysis further demonstrated that the four Cyber Resilience dimensions collectively explained 82.8% of the

variance in Business Continuity ($R^2 = 0.828$, Adjusted $R^2 = 0.826$), and the overall regression model was statistically significant, $F(4,379) = 456.084$, $p < 0.001$.

Furthermore, Threat Detection, Incident Response, Recovery Capability, and Security Awareness were all statistically significant positive predictors of Business Continuity. Therefore, H1, H1a, H1b, H1c, and H1d were supported.

Overall, the findings provide empirical support for the proposed research model and indicate that stronger Cyber Resilience Capabilities are associated with stronger Business Continuity among the organizations represented in the study.

5. Chapter five: Research limitations, Recommendations & Conclusion

5.1. Research Limitations & Future Research

5.1.1 Research Limitations

Although this study provides useful findings regarding the relationship between Cyber Resilience Capabilities and Business Continuity in Saudi organizations, several limitations should be acknowledged.

First, the study was conducted using a quantitative, cross-sectional research design. Data were collected at a single point in time; therefore, the study provides an assessment of the relationship between Cyber Resilience Capabilities and Business Continuity but does not capture how these capabilities or their effects may change over time.

Second, the study relied on a structured self-reported questionnaire. Although the questionnaire demonstrated excellent overall reliability, with a Cronbach's Alpha of 0.952, respondents' answers may be influenced by individual perceptions, experiences, or organizational circumstances. Consequently, some degree of response or perception bias may exist.

Third, the study focused on Saudi organizations, which limits the generalizability of the findings to organizations operating in other countries or different regulatory and technological environments. Cybersecurity practices and business continuity requirements may vary depending on national regulations, organizational size, industry, and technological maturity.

Fourth, the study examined Cyber Resilience Capabilities through four dimensions—Threat Detection, Incident Response, Recovery Capability, and Security Awareness—and Business Continuity through Operational Continuity, Service Availability, Recovery Speed, and Organizational Stability. Other

organizational, technological, environmental, and managerial factors that may influence business continuity were outside the scope of this study.

Finally, the statistical analysis identified a very strong positive relationship between Cyber Resilience Capabilities and Business Continuity ($r = 0.909$, $p < 0.001$) and indicated that Cyber Resilience Capabilities explained 82.8% of the variance in Business Continuity ($R^2 = 0.828$). However, the remaining 17.2% suggests that other factors not examined in this study may also contribute to differences in Business Continuity performance.

5.1.2 Future Research

Future research can address these limitations by adopting a longitudinal research design to examine how Cyber Resilience Capabilities and Business Continuity develop over time, particularly before and after significant cybersecurity incidents.

Future studies could also use mixed-method or qualitative approaches, including interviews with cybersecurity professionals, managers, and business continuity specialists. This would provide deeper insights into the organizational practices and challenges underlying the statistical relationships identified in this study.

Researchers may also expand the geographical scope by comparing Saudi organizations with organizations in other countries or regions. Comparative studies could examine how differences in regulations, cybersecurity maturity, organizational culture, and industry characteristics influence cyber resilience and business continuity.

In addition, future research could examine other factors that may influence Business Continuity, such as organizational leadership, cybersecurity investment, employee training, risk management maturity, digital transformation, and organizational culture. Examining these factors alongside Cyber Resilience Capabilities could

provide a more comprehensive understanding of the determinants of Business Continuity.

Finally, future studies could investigate the individual dimensions of Cyber Resilience Capabilities separately to determine which capability has the greatest influence on Business Continuity. This could help organizations prioritize their cybersecurity investments and develop more targeted resilience strategies.

5.2. Research Recommendations

Based on the findings of this study, several recommendations are proposed to help Saudi organizations strengthen their Cyber Resilience Capabilities and improve Business Continuity.

5.2.1 Strengthen Threat Detection Capabilities

Organizations should invest in advanced cybersecurity monitoring and threat detection mechanisms to identify potential cyber threats at an early stage. Continuous monitoring, automated alerts, vulnerability assessments, and regular security assessments can help organizations detect suspicious activities before they develop into major disruptions.

5.2.2 Improve Incident Response Procedures

Organizations should establish and regularly update formal incident response plans that clearly define responsibilities, communication procedures, escalation processes, and response actions. Regular cybersecurity incident simulations and exercises should also be conducted to ensure that employees and responsible teams can respond effectively when incidents occur.

5.2.3 Enhance Recovery Capabilities

Organizations should strengthen their ability to recover critical systems and services following cybersecurity incidents. This includes maintaining regular backups, establishing recovery procedures, testing disaster recovery plans, and ensuring that critical systems can be restored within an acceptable period.

5.2.4 Increase Cybersecurity Awareness

Organizations should provide continuous cybersecurity awareness and training programs for employees. Training should address common cyber threats such as phishing, social engineering, password-related risks, and inappropriate handling of sensitive information. Regular awareness activities can help develop a stronger security culture throughout the organization.

5.2.5 Integrate Cybersecurity with Business Continuity Planning

Cybersecurity should be integrated into existing Business Continuity Management Systems (BCMS) rather than being treated as a separate technical function. Business continuity plans should consider potential cyber incidents and define how critical operations, services, and information systems will be maintained during and after a cybersecurity disruption.

5.2.6 Conduct Regular Resilience Testing

Organizations should regularly test their cybersecurity and business continuity arrangements through simulations, scenario-based exercises, and recovery drills. These activities can identify weaknesses in existing procedures and allow organizations to improve their preparedness before an actual disruption occurs.

5.2.7 Establish Continuous Monitoring and Improvement

Cyber resilience should be treated as a continuous organizational process rather than a one-time initiative. Organizations should regularly assess their cybersecurity capabilities, review incident experiences, monitor emerging threats, and update their policies and procedures accordingly.

5.2.8 Strengthen Management Support and Investment

Senior management should provide adequate financial, technological, and human resources for cybersecurity and business continuity initiatives. Management commitment is essential for ensuring that cyber resilience becomes an organizational priority and that the necessary resources are available to maintain and improve resilience capabilities.

Overall Recommendation

Overall, Saudi organizations should adopt a proactive and integrated approach in which threat detection, incident response, recovery, and cybersecurity awareness are closely connected with Business Continuity planning. The very strong positive

relationship identified in this study ($r = 0.909$, $p < 0.001$) and the high explanatory power of the regression model ($R^2 = 0.828$) highlight the importance of strengthening Cyber Resilience Capabilities as part of broader organizational continuity and resilience strategies.

5.3. Conclusion

This study examined the relationship between Cyber Resilience Capabilities and Business Continuity in Saudi organizations. The study adopted a quantitative cross-sectional research design and analyzed 384 valid questionnaire responses. Cyber Resilience Capabilities were examined through four dimensions: Threat Detection, Incident Response, Recovery Capability, and Security Awareness, while Business Continuity was measured through Operational Continuity, Service Availability, Recovery Speed, and Organizational Stability.

The reliability analysis demonstrated excellent overall internal consistency, with a Cronbach's Alpha of 0.952. The descriptive findings indicated generally positive perceptions of both Cyber Resilience Capabilities and Business Continuity. Recovery Capability recorded the highest mean among the Cyber Resilience dimensions ($M = 3.985$), while Recovery Speed recorded the highest mean among the Business Continuity dimensions ($M = 3.993$).

The inferential analysis provided strong evidence of the relationship between the two main research variables. Pearson correlation analysis identified a very strong positive and statistically significant relationship between Cyber Resilience Capabilities and Business Continuity ($r = 0.909$, $p < 0.001$). Multiple regression analysis demonstrated that the four Cyber Resilience dimensions collectively explained 82.8% of the variance in Business Continuity ($R^2 = 0.828$, Adjusted $R^2 =$

0.826), with the overall model being statistically significant, $F(4,379) = 456.084$, $p < 0.001$.

Furthermore, Threat Detection, Incident Response, Recovery Capability, and Security Awareness were all significant positive predictors of Business Continuity. Accordingly, H1, H1a, H1b, H1c, and H1d were supported.

Overall, the findings indicate that organizations represented in the study with stronger Cyber Resilience Capabilities also reported stronger Business Continuity. The results emphasize the importance of developing an integrated approach to cybersecurity resilience that combines effective threat detection, incident response, recovery capabilities, and employee security awareness with business continuity planning. The study therefore contributes empirical evidence regarding the role of Cyber Resilience Capabilities in supporting Business Continuity within the Saudi organizational context.

References

- IBM Security. (2024). *Cost of a Data Breach Report 2024*. IBM Corporation.
- International Organization for Standardization (ISO). (2019). *ISO 22301: Security and resilience—Business continuity management systems—Requirements*. ISO.
- Linkov, I., & Kott, A. (2019). *Fundamental concepts of cyber resilience: Introduction and overview*. In I. Linkov & A. Kott (Eds.), *Cyber Resilience of Systems and Networks* (pp. 1–25). Springer.
- National Institute of Standards and Technology (NIST). (2024). *Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce.
- Saudi Data and Artificial Intelligence Authority (SDAIA). (2024). *Digital Transformation and Cybersecurity Initiatives Report*. Riyadh, Saudi Arabia.
- World Economic Forum. (2024). *Global Cybersecurity Outlook 2024*. World Economic Forum.
- Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). *Cyber security awareness campaigns: Why do they fail to change behaviour?* *arXiv Preprint arXiv:1901.02672*.
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide (SP 800-61 Rev. 2)*. National Institute of Standards and Technology.
- Herbane, B. (2010). *Small business research: Time for a crisis-based view*. *International Small Business Journal*, 28(1), 43–64.
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). *Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)*. *Computers & Security*, 42, 165–176.
- Von Solms, R., & Van Niekerk, J. (2013). *From information security to cyber security*. *Computers & Security*, 38, 97–102.
- Creswell, J. W., & Creswell, J. D. (2023). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (7th ed.)*. SAGE Publications.
- Saunders, M., Lewis, P., & Thornhill, A. (2023). *Research Methods for Business Students (9th ed.)*. Pearson.
- Sekaran, U., & Bougie, R. (2020). *Research Methods for Business: A Skill-Building Approach (8th ed.)*. Wiley.

- *Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. Educational and Psychological Measurement, 30(3), 607–610.*
- *Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2022). Multivariate data analysis (9th ed.). Cengage Learning.*

Appendix

APPENDIX A

Questionnaire

Research Title

The Impact of Cyber Resilience Capabilities on Business Continuity in Saudi Organizations

Dear Participant,

I am conducting this questionnaire for academic purposes as part of a graduation project. The purpose of this study is to examine the impact of Cyber Resilience Capabilities on Business Continuity in Saudi Organizations.

Your participation is highly appreciated. All responses will remain confidential and will be used solely for research purposes. There are no right or wrong answers. Please answer honestly based on your experience and perception.

Response Scale

Please indicate your level of agreement with the following statements using the scale below:

Scale	Description
1	Strongly Disagree
2	Disagree
3	Neutral
4	Agree
5	Strongly Agree

Section A: Demographic Information

1. Gender

- Male
- Female

2. Age

- Less than 25 years
- 25–34 years
- 35–44 years
- 45–54 years
- 55 years and above

3. Educational Qualification

- Diploma
- Bachelor's Degree
- Master's Degree
- Doctorate
- Other

4. Job Position

- Employee
- Supervisor
- Manager
- Senior Manager
- Other

5. Years of Experience

- Less than 5 years
- 5–10 years
- 11–15 years
- 16–20 years
- More than 20 years

Section B: Cyber Resilience Capabilities (Independent Variable)

Dimension 1: Threat Detection

1. Our organization continuously monitors cybersecurity threats.
2. Potential cyber threats are detected at an early stage.
3. Security monitoring systems are effective in identifying risks.
4. Threat intelligence information is regularly utilized.
5. Cybersecurity vulnerabilities are identified before causing major damage.

Dimension 2: Incident Response

6. The organization has a clear cyber incident response plan.
7. Employees understand their responsibilities during cyber incidents.
8. Cybersecurity incidents are managed effectively.
9. Response teams react quickly to cybersecurity incidents.
10. Incident response procedures are regularly tested and updated.

Dimension 3: Recovery Capability

11. Critical systems can be restored quickly after cyber incidents.
12. Backup and recovery procedures are effective.
13. Business operations can continue during cyber disruptions.
14. Recovery plans are clearly documented.
15. Recovery processes minimize operational downtime.

Dimension 4: Security Awareness

16. Employees receive regular cybersecurity training.
17. Employees understand organizational cybersecurity policies.
18. The organization promotes cybersecurity awareness.
19. Employees can recognize common cyber threats such as phishing.
20. Security awareness programs improve cybersecurity behavior.

Section C: Business Continuity (Dependent Variable)

Dimension 1: Operational Continuity

- 21. Critical business operations continue during disruptions.
- 22. The organization can maintain essential activities during cyber incidents.
- 23. Operational interruptions are minimized during disruptions.
- 24. Business processes remain functional under adverse conditions.
- 25. The organization can sustain operations during emergencies.

Dimension 2: Service Availability

- 26. Essential services remain available during cyber incidents.
- 27. Customers can access critical services during disruptions.
- 28. Service interruptions are minimized.
- 29. Technology systems support continuous service delivery.
- 30. The organization maintains acceptable service levels during crises.

Dimension 3: Recovery Speed

- 31. The organization recovers quickly after cyber incidents.
- 32. Recovery objectives are achieved within expected timeframes.
- 33. Downtime is minimized following disruptions.
- 34. Systems and services are restored efficiently.
- 35. Recovery procedures support rapid resumption of operations.

Dimension 4: Organizational Stability

36. The organization remains stable during cyber disruptions.

37. Employees adapt effectively to unexpected incidents.

38. Stakeholder confidence is maintained during crises.

39. The organization can withstand major cyber disruptions.

40. Business continuity planning contributes to long-term organizational stability.

Thank you for your valuable participation.

Table 1: Research Instruments

Variable	Dimension	Number of Items	Item Numbers	Reference
Cyber Resilience Capabilities	Threat Detection	5	1–5	NIST (2024)
Cyber Resilience Capabilities	Incident Response	5	6–10	Cichonski et al. (2012)
Cyber Resilience Capabilities	Recovery Capability	5	11–15	ISO 22301 (2019)
Cyber Resilience Capabilities	Security Awareness	5	16–20	Parsons et al. (2014)
Business Continuity	Operational Continuity	5	21–25	ISO 22301 (2019)
Business Continuity	Service Availability	5	26–30	Herbane (2010)
Business Continuity	Recovery Speed	5	31–35	ISO 22301 (2019)

Business Continuity	Organizational Stability	5	36–40	Linkov & Kott (2019)
---------------------	--------------------------	---	-------	----------------------

Total Number of Questionnaire Items = 40

Questionnaire Scale = Five-Point Likert Scale

1 = Strongly Disagree

2 = Disagree

3 = Neutral

4 = Agree

5 = Strongly Agree

Source: Developed by the Researcher (2026).

Google Form Link:

<https://forms.gle/81wEvhkyeWxaSEv88>