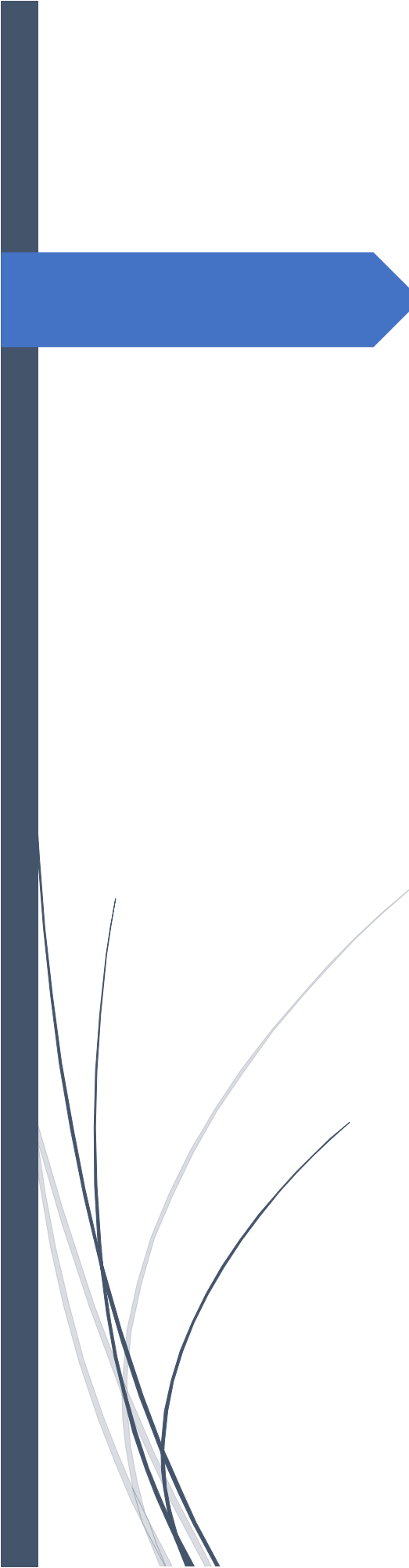




# Final Project 2

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

27/06/2026 – Second Trimester 2026

# Abstract

## **Purpose:**

This study aims to examine the impact of Cyber Resilience on Business Continuity in Saudi organizations. As organizations increasingly rely on digital technologies and interconnected systems, cyber threats have become one of the most significant challenges affecting operational stability and organizational performance. Therefore, the ability of organizations to prepare for, detect, respond to, and recover from cyber incidents has become essential for ensuring business continuity. This research investigates the extent to which cyber resilience contributes to maintaining continuous operations and minimizing disruptions caused by cybersecurity incidents.

## **Methodology:**

The study adopts a quantitative research approach using a structured questionnaire distributed to employees and managers working in Saudi organizations across different sectors. The questionnaire measures Cyber Resilience as the independent variable through four dimensions: Threat Detection, Incident Response, Recovery Capability, and Security Awareness. Business Continuity is measured as the dependent variable through four dimensions: Operational Continuity, Service Availability, Recovery Speed, and Organizational Stability. Data will be analyzed using statistical techniques through SPSS software to examine the relationship between the study variables and test the proposed hypotheses.

## **Findings:**

The study expects to identify a positive and statistically significant relationship between Cyber Resilience and Business Continuity. Organizations with stronger cyber resilience capabilities are anticipated to demonstrate higher levels of operational continuity, faster recovery from cyber incidents, improved service availability, and greater organizational stability during disruptions.

## **Originality & Implication:**

This research contributes to the growing body of knowledge on cybersecurity management and organizational resilience by examining cyber resilience within the Saudi organizational context. The findings are expected to provide practical insights for decision-makers, managers, and policymakers regarding the importance of strengthening cyber resilience strategies to enhance business continuity and organizational sustainability.

**Keywords:** *Cyber Resilience, Business Continuity, Cybersecurity, Incident Response, Recovery Capability, Organizational Stability, Saudi Organizations.*

# Table of Contents

|                                                                                |    |
|--------------------------------------------------------------------------------|----|
| Abstract .....                                                                 | 2  |
| 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 |

|             |                                                                                       |           |
|-------------|---------------------------------------------------------------------------------------|-----------|
| <b>3.1.</b> | <b>Introduction .....</b>                                                             | <b>29</b> |
| <b>3.2.</b> | <b>Operational definitions for research variables .....</b>                           | <b>31</b> |
| –           | <b>Cyber Resilience Capabilities (Independent Variable) .....</b>                     | <b>31</b> |
|             | Threat Detection.....                                                                 | 31        |
|             | Incident Response .....                                                               | 32        |
|             | Recovery Capability.....                                                              | 32        |
|             | Security Awareness.....                                                               | 32        |
| –           | <b>Business Continuity (Dependent Variable).....</b>                                  | <b>33</b> |
|             | Operational Continuity.....                                                           | 33        |
|             | Service Availability .....                                                            | 33        |
|             | Recovery Speed .....                                                                  | 33        |
|             | Organizational Stability .....                                                        | 34        |
| <b>3.3.</b> | <b>Research design (research onion).....</b>                                          | <b>34</b> |
| <b>3.4.</b> | <b>Research population &amp; Sampling methods and technique .....</b>                 | <b>38</b> |
| <b>3.5.</b> | <b>Data collection method .....</b>                                                   | <b>42</b> |
| <b>3.6.</b> | <b>Types of data .....</b>                                                            | <b>44</b> |
| <b>3.7.</b> | <b>Statistical analysis procedures.....</b>                                           | <b>47</b> |
| <b>3.8.</b> | <b>Conclusion .....</b>                                                               | <b>50</b> |
| <b>4.</b>   | <b>Chapter 4: Statistical Analysis &amp; Findings discussion .....</b>                | <b>52</b> |
| <b>4.1.</b> | <b>Introduction .....</b>                                                             | <b>53</b> |
| <b>4.2.</b> | <b>Sample profile (descriptive statistics for research sample).....</b>               | <b>54</b> |
| <b>4.3.</b> | <b>Validity &amp; reliability tests for the questionnaires.....</b>                   | <b>57</b> |
| <b>4.4.</b> | <b>Descriptive statistics for research variables (answer research questions).....</b> | <b>57</b> |
| <b>4.5.</b> | <b>Testing Hypotheses &amp; Findings Discussion .....</b>                             | <b>58</b> |
| <b>4.6.</b> | <b>Conclusion .....</b>                                                               | <b>58</b> |
| <b>5.</b>   | <b>Chapter five: Research limitations, Recommendations &amp; Conclusion .....</b>     | <b>59</b> |
| <b>5.1.</b> | <b>Research Limitations &amp; Future Research .....</b>                               | <b>60</b> |
| <b>5.2.</b> | <b>Research Recommendations .....</b>                                                 | <b>60</b> |
|             | <b>References.....</b>                                                                | <b>62</b> |
|             | <b>Appendix.....</b>                                                                  | <b>64</b> |

## **List of Figures:**

|                                                         |           |
|---------------------------------------------------------|-----------|
| <b>Figure 1.1 Research Model .....</b>                  | <b>18</b> |
| <b>Figure 1.2: Project Structure.....</b>               | <b>20</b> |
| <b>Figure 3.1: Research Onion of the Study.....</b>     | <b>37</b> |
| <b>Figure 3.2: Sampling Procedure of the Study.....</b> | <b>41</b> |

## **List of Tables:**

|                                                                                  |           |
|----------------------------------------------------------------------------------|-----------|
| <b>Table 3.1: Operational Definitions of the Research Variables .....</b>        | <b>31</b> |
| <b>Table 3.2: Research Design Summary.....</b>                                   | <b>37</b> |
| <b>Table 3.3: Population and Sampling Summary.....</b>                           | <b>40</b> |
| <b>Table 3.4: Five-Point Likert Scale Used in the Study .....</b>                | <b>43</b> |
| <b>Table 3.5: Structure of the Research Questionnaire .....</b>                  | <b>44</b> |
| <b>Table 3.6: Types of Data Used in the Study.....</b>                           | <b>46</b> |
| <b>Table 3.7: Statistical Analysis Procedures.....</b>                           | <b>49</b> |
| <b>Table 4.1: Distribution of Respondents by Gender .....</b>                    | <b>55</b> |
| <b>Table 4.2: Distribution of Respondents by Age .....</b>                       | <b>55</b> |
| <b>Table 4.3: Distribution of Respondents by Educational Qualification .....</b> | <b>55</b> |
| <b>Table 4.4: Distribution of Respondents by Job Position.....</b>               | <b>56</b> |
| <b>Table 4.5: Distribution of Respondents by Years of Experience .....</b>       | <b>56</b> |

# **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 (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, 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.

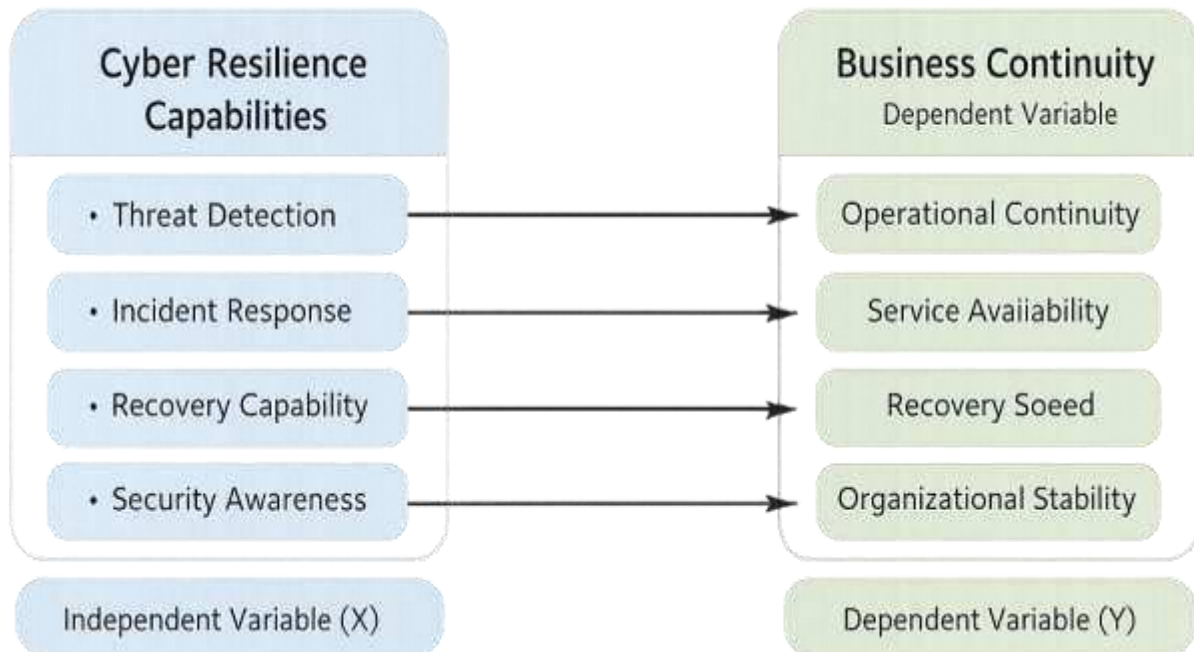
H01c: There is no statistically significant impact of Recovery Capability on Business Continuity.

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.

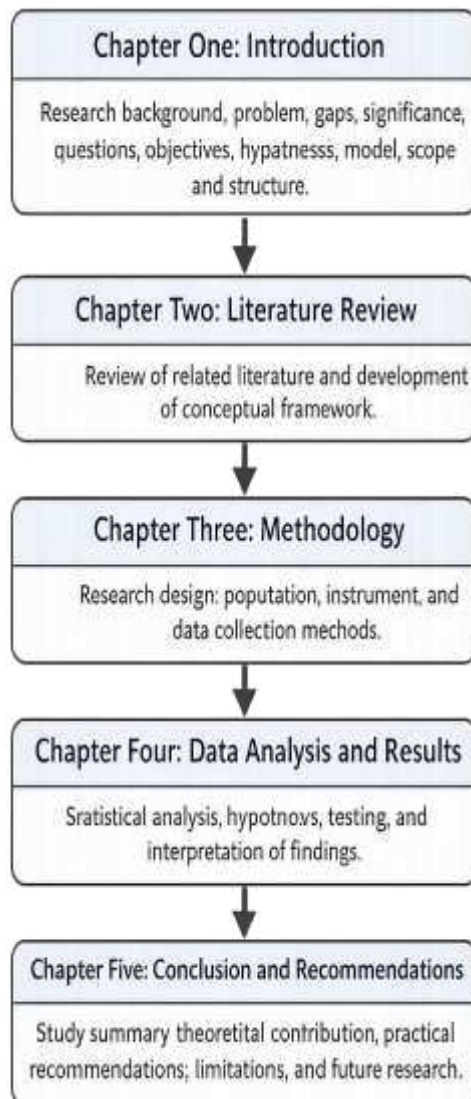
Chapter One presents the introduction of the study, including the research background, research problem, theoretical and practical gaps, research significance, research questions, research objectives, research hypotheses, research model, scope of the study, and project structure.

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.

This study adopts a quantitative research approach, 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 is employed as the primary instrument for data collection, allowing respondents to express their perceptions regarding cyber resilience capabilities and business continuity practices within their organizations. The collected data will be 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 consists 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 is adopted to facilitate data collection from participants who are readily accessible and willing to participate in the study. The questionnaire will be distributed electronically through Google Forms, enabling efficient data collection while maintaining respondent confidentiality.

Furthermore, this chapter explains the statistical procedures that will be applied after data collection. These procedures include 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 impact of Cyber Resilience Capabilities on Business Continuity. The results of these analyses will provide 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                                                           |
|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| <b>Cyber Resilience Capabilities (Independent Variable)</b> | 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) |
| <b>Business Continuity (Dependent Variable)</b>             | 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 will be collected using a structured online questionnaire developed based on previous literature and internationally recognized cybersecurity frameworks. The questionnaire consists 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             |

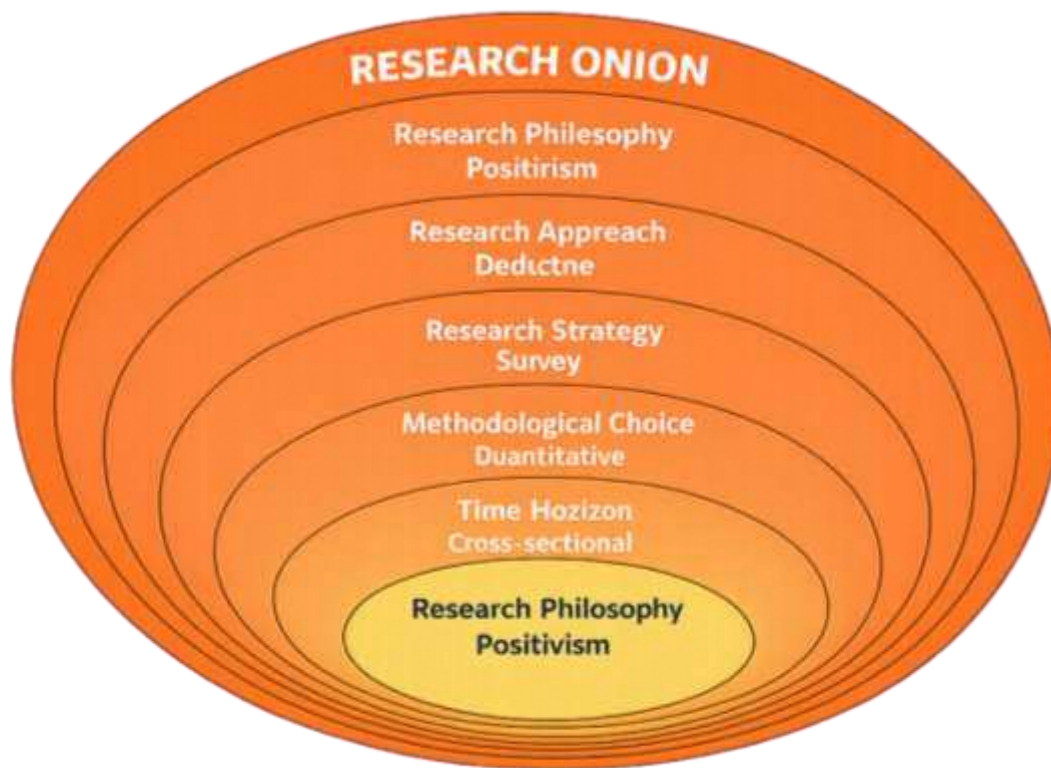


Figure 3.1: Research Onion of the Study

### **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 will be distributed electronically using Google Forms through professional networks, organizational contacts, email communication, and social media platforms. Participation in the survey is entirely voluntary, and respondents will be informed that all collected information will remain confidential and 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.

Accordingly, this research aims to collect at least 384 valid responses from employees working in Saudi organizations. Obtaining a sample of this size will provide sufficient statistical power to perform descriptive analysis, reliability testing, correlation analysis, and multiple regression analysis using SPSS.

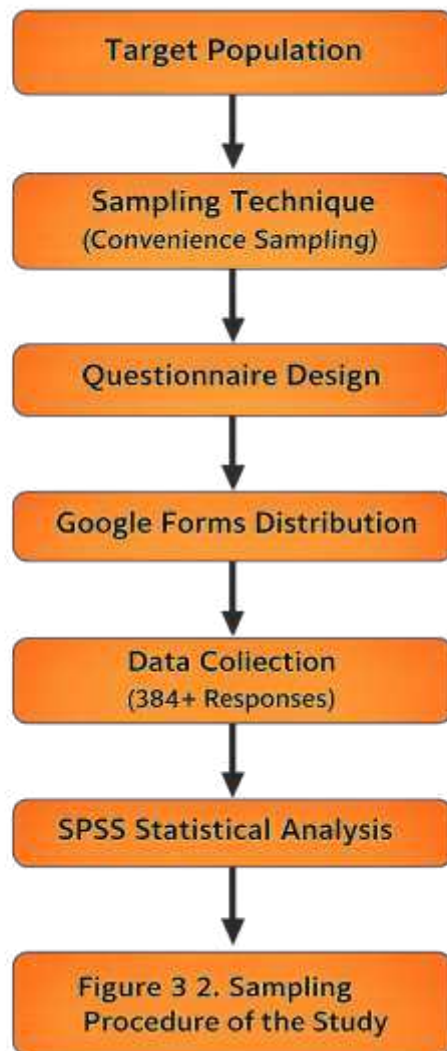
*Table 3.3: Population and Sampling Summary*

| <b>Item</b>            | <b>Description</b>                       |
|------------------------|------------------------------------------|
| 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)      |
| Target Sample Size     | Minimum 384 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 will be 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 will be created and distributed electronically using Google Forms, which provides an efficient, secure, and user-friendly platform for collecting research data. The survey link will be shared through professional networks, organizational contacts, email communication, and social media platforms to reach employees working in Saudi organizations. Respondents will be informed that participation is voluntary and that all responses will remain anonymous and confidential. No personally identifiable information will be collected, and the data will be used exclusively for academic research purposes.

Prior to the official distribution of the questionnaire, the instrument will undergo a pilot review to ensure that the wording of the questions is clear, understandable, and relevant to the research objectives. Feedback obtained during this stage will be

incorporated to improve the quality and clarity of the questionnaire before launching the final survey.

After the data collection period has ended, all valid responses will be exported from Google Forms into Microsoft Excel and subsequently imported into the Statistical Package for the Social Sciences (SPSS) Version 29 for coding, data cleaning, and statistical analysis. The collected data will then be 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               |
| Section B    | Cyber Resilience Capabilities | 20              |
| Section C    | Business Continuity           | 20              |
| <b>Total</b> | <b>Questionnaire Items</b>    | <b>45</b>       |

### **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 will be 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 will evaluate each statement using a five-point Likert Scale ranging from Strongly Disagree (1) to Strongly Agree (5). The collected responses will provide 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*

| <b>Data Type</b>      | <b>Source</b>                                                                                                            | <b>Purpose</b>                                                                    |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| <b>Primary Data</b>   | Online questionnaire (Google Forms) completed by employees working in Saudi organizations                                | Measure Cyber Resilience Capabilities and Business Continuity                     |
| <b>Secondary Data</b> | 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 will be exported from Google Forms into Microsoft Excel for preliminary data screening. The cleaned dataset will then be imported into the Statistical Package for the Social Sciences (SPSS) Version 29 for coding, processing, and statistical analysis.

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

- **Descriptive Statistics**

Descriptive statistics will be used to summarize the demographic characteristics of the respondents, including gender, age, educational qualification, job position, and years of experience. In addition, descriptive statistics will be calculated for all 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 will be 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 will be reviewed by academic supervisors to ensure that the measurement items accurately represent the research variables and objectives.

- **Correlation Analysis**

Pearson Correlation Analysis will be 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 will be employed to determine the effect of the four dimensions of Cyber Resilience Capabilities—Threat Detection, Incident Response, Recovery Capability, and Security Awareness—on 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 will be tested using regression analysis based on a significance level ( $\alpha$ ) of 0.05. If the probability value (p-value) is less than 0.05, the null hypothesis will be rejected, indicating a statistically significant relationship between the variables. Conversely, if the p-value is greater than 0.05, the null hypothesis will not be 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 will be 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 impact of Cyber Resilience Capabilities on Business Continuity in Saudi organizations. It described the overall methodological framework, including the operational definitions of the research variables, research design, target population, sampling technique, data collection procedures, types of data, and statistical analysis methods that will be employed to achieve the research objectives.

The study adopts a quantitative research approach based on the positivism research philosophy and the deductive research approach, using a survey strategy to collect

empirical data from employees working in Saudi organizations. A structured questionnaire consisting of demographic questions and measurement items related to the research variables will be distributed electronically through Google Forms. The questionnaire is designed to measure the dimensions of Cyber Resilience Capabilities and Business Continuity using a five-point Likert scale.

The chapter also explained the sampling method and justified the selection of a non-probability convenience sampling technique. Furthermore, the statistical procedures that will be performed using **SPSS Version 29** were discussed, including descriptive statistics, reliability analysis using Cronbach's Alpha, Pearson correlation analysis, and multiple regression analysis. These statistical techniques are appropriate for examining the relationships among the research variables and testing the proposed hypotheses.

Overall, the methodology adopted in this study provides a systematic and scientifically accepted approach for collecting, analyzing, and interpreting the research data. The selected methods are expected to produce reliable and valid findings that contribute to understanding how cyber resilience capabilities influence business continuity within Saudi organizations.

The following chapter presents the statistical analysis of the collected data, beginning with the demographic characteristics of the respondents, followed by descriptive statistics, reliability analysis, correlation analysis, regression analysis, hypothesis testing, and a discussion of the research findings.

## **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 is conducted using the Statistical Package for the Social Sciences (SPSS) Version 29, which provides a comprehensive set of statistical techniques for organizing, analyzing, and interpreting quantitative research data.

This chapter begins by presenting the demographic characteristics of the 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 and help determine whether the collected data adequately represent the target population.

Following the demographic analysis, descriptive statistics will be presented to summarize the respondents' perceptions regarding the research variables, namely Cyber Resilience Capabilities and Business Continuity. The statistical analysis will include measures such as frequencies, percentages, means, and standard deviations to provide an overall understanding of the collected data.

The reliability of the research instrument will be evaluated using Cronbach's Alpha Coefficient to assess the internal consistency of the questionnaire items. Correlation analysis will then be conducted to examine the strength and direction of the relationships between the research variables. Finally, multiple regression analysis will be performed to investigate the impact of Cyber Resilience Capabilities on Business Continuity and to test the proposed research hypotheses.

Since the present assignment represents the methodology and preparation stage of the research, this chapter includes the structure of the statistical analysis and the

demographic profile of the respondents. The remaining statistical analyses and hypothesis testing will be completed after the required number of questionnaire responses has been collected and processed using SPSS.

Overall, this chapter provides the analytical framework for interpreting the research data and forms the basis for discussing the findings and drawing conclusions regarding the impact of Cyber Resilience Capabilities on Business Continuity in Saudi organizations.

#### **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 will be 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*

| <b>Gender</b> | <b>Frequency</b> | <b>Percentage (%)</b> |
|---------------|------------------|-----------------------|
| Male          | —                | —                     |
| Female        | —                | —                     |
| <b>Total</b>  | —                | <b>100%</b>           |

*Table 4.2: Distribution of Respondents by Age*

| <b>Age Group</b>   | <b>Frequency</b> | <b>Percentage (%)</b> |
|--------------------|------------------|-----------------------|
| Less than 25 years | —                | —                     |
| 25–34 years        | —                | —                     |
| 35–44 years        | —                | —                     |
| 45–54 years        | —                | —                     |
| 55 years and above | —                | —                     |
| <b>Total</b>       | —                | <b>100%</b>           |

*Table 4.3: Distribution of Respondents by Educational Qualification*

| <b>Educational Qualification</b> | <b>Frequency</b> | <b>Percentage (%)</b> |
|----------------------------------|------------------|-----------------------|
| Diploma                          | —                | —                     |
| Bachelor's Degree                | —                | —                     |
| Master's Degree                  | —                | —                     |
| Doctorate                        | —                | —                     |
| Other                            | —                | —                     |
| <b>Total</b>                     | —                | <b>100%</b>           |

*Table 4.4: Distribution of Respondents by Job Position*

| <b>Job Position</b> | <b>Frequency</b> | <b>Percentage (%)</b> |
|---------------------|------------------|-----------------------|
| Employee            | —                | —                     |
| Supervisor          | —                | —                     |
| Manager             | —                | —                     |
| Senior Manager      | —                | —                     |
| Executive Manager   | —                | —                     |
| Other               | —                | —                     |
| <b>Total</b>        | —                | <b>100%</b>           |

*Table 4.5: Distribution of Respondents by Years of Experience*

| <b>Years of Experience</b> | <b>Frequency</b> | <b>Percentage (%)</b> |
|----------------------------|------------------|-----------------------|
| Less than 5 years          | —                | —                     |
| 5–10 years                 | —                | —                     |
| 11–15 years                | —                | —                     |
| 16–20 years                | —                | —                     |
| More than 20 years         | —                | —                     |
| <b>Total</b>               | —                | <b>100%</b>           |

## **Discussion**

The demographic information presented in the above tables provides a comprehensive overview of the respondents participating in this study. These characteristics are important because they help determine whether the research sample represents different categories of employees working in Saudi organizations. Once the questionnaire responses are collected, the frequency and percentage values generated by SPSS will be inserted into these tables and interpreted accordingly.

The demographic analysis serves as the foundation for the subsequent statistical analyses presented in this chapter. Following the sample profile, descriptive statistics, reliability analysis, correlation analysis, and multiple regression analysis will be conducted to examine the relationship between Cyber Resilience Capabilities and Business Continuity.

#### **4.3. Validity & reliability tests for the questionnaires**

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

## **4.5.     Testing Hypotheses & Findings Discussion**

## **4.6.     Conclusion**

## **5. Chapter five: Research limitations, Recommendations & Conclusion**

## **5.1. Research Limitations & Future Research**

## **5.2. Research Recommendations**

## **5.3. Conclusion**



## 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.
- Ross, R., McEvilly, M., & Oren, J. (2016). *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*. NIST Special Publication 800-160.
- 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.*
- *ISO. (2019). ISO 22301: Security and resilience—Business continuity management systems—Requirements.*
- *NIST. (2024). Cybersecurity Framework (CSF) 2.0.*
- *Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. Educational and Psychological Measurement, 30(3), 607–610.*

# 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**

| <b>Variable</b>               | <b>Dimension</b>         | <b>Number of Items</b> | <b>Item Numbers</b> | <b>Reference</b>        |
|-------------------------------|--------------------------|------------------------|---------------------|-------------------------|
| 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>