

Final Project 2

PMG 497

Project Template

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

13/06/2026 – 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	3
1. Chapter 1: Introduction	6
1.1. Research Background	7
1.2. Research Problem.....	10
1.2.1. Theoretical Gaps	11
1.2.2. Practical Gaps.....	12
1.3. Research Significance.....	13
1.3.1. At the theoretical level	13
1.3.2. At the practical level	14
1.4. Research Questions	15
1.5. Research Objectives	15
1.6. Research Hypotheses.....	16
1.7. Research Model	17
1.8. Scope of The Study	17
1.9. The Project Structure.....	18
2. Chapter 2: Literature Review.....	20
2.1. Introduction	21
2.2. The independent variable	22
2.2.1 Threat Detection.....	22
2.2.2 Incident Response	23
2.2.3 Recovery Capability.....	23
2.2.4 Security Awareness	23
2.3. The dependent variable.....	24
2.3.1 Operational Continuity.....	24
2.3.2 Service Availability	24
2.3.3 Recovery Speed	24
2.3.4 Organizational Stability	25
2.4. The relationship between the independent and the dependent variables.....	25
2.5. Conclusion	26
3. Chapter 3: Research Methodology.....	27

3.1.	Introduction	28
3.2.	Operational definitions for research variables	28
3.3.	Research design (research onion).....	28
3.4.	Research population & Sampling methods and technique	29
3.5.	Data collection method	30
3.6.	Types of data	30
3.7.	Statistical analysis procedures.....	30
3.8.	Conclusion	31
4.	Chapter 4: Statistical Analysis & Findings discussion	32
4.1.	Introduction	33
4.2.	Sample profile (descriptive statistics for research sample).....	33
4.3.	Validity & reliability tests for the questionnaires.....	33
4.4.	Descriptive statistics for research variables (answer research questions).....	34
4.5.	Testing Hypotheses & Findings Discussion	34
4.6.	Conclusion	35
5.	Chapter five: Research limitations, Recommendations & Conclusion	36
5.1.	Research Limitations & Future Research.....	37
5.2.	Research Recommendations	37
	References.....	38
	Appendix.....	40

List of Figures:

Figure 1.1 Research Model.....	17
Figure 1.2: Project Structure	19

List of Tables:

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

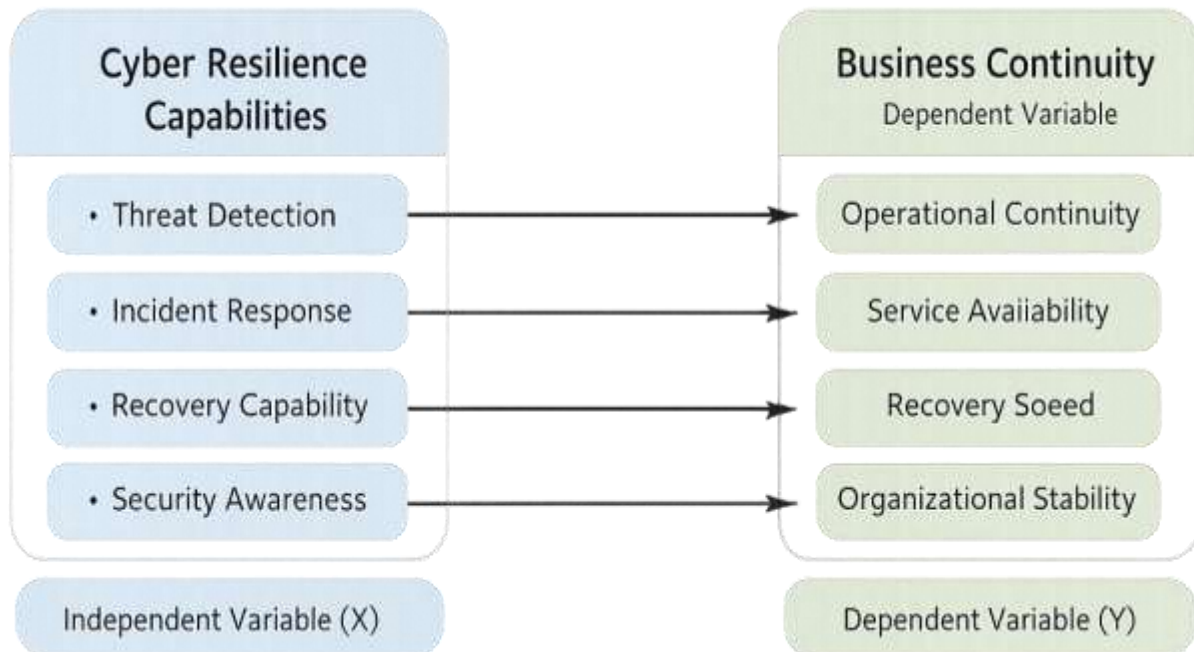


Figure 1.1 Research Model

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.

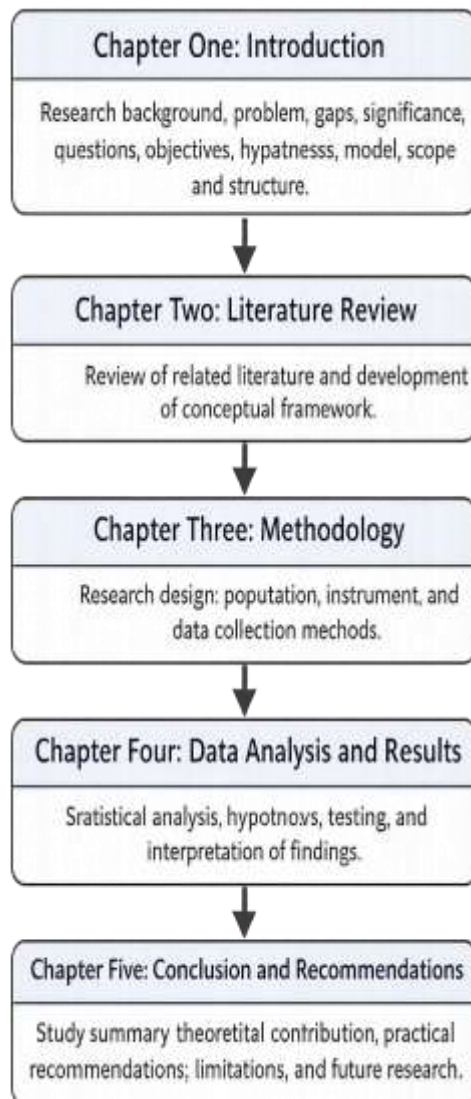


Figure 1.2: Project Structure

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

3.2. Operational definitions for research variables

3.3. Research design (research onion)

3.4. Research population & Sampling methods and technique

3.5. Data collection method

3.6. Types of data

3.7. Statistical analysis procedures

3.8. Conclusion

4. Chapter 4: Statistical Analysis & Findings discussion

4.1. Introduction

4.2. Sample profile (descriptive statistics for research sample)

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., McEvilley, 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.

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>