



Research Proposal

Developing a Cybersecurity Risk Assessment Framework for Mitigating Spear-Phishing Attacks Against Airline Employees

Submitted By

Abdullah Al Noman

Student ID:

2520302

Module

Research Methods and Professional Development

(ACFA7004_LON)

Department

MSC Cybersecurity and Digital Forensics

Table of Contents	Page
1. Introduction	3
1.1 Context and Background	3
1.2 Research Problem	3
1.3 Research Aim and Objectives	4
1.4 Significance of the Research	5
2. Literature Review	5
2.1 Introduction	5
2.2 Aviation Cybersecurity	5
2.3 Spear-Phishing Attacks	6
2.4 Human Factors in Cybersecurity	6
2.5 Cybersecurity Risk Assessment Frameworks	7
2.6 Research Gap	8
3. Research Design and Methodology	8
3.1 Introduction	
3.2 Research Philosophy	8
3.3 Research Approach	9
3.4 Research Design	10
3.5 Research Method	10
3.6 Data Collection and Analysis	11
3.7 Framework Development Process	12
3.8 Framework Development Process	12
3.9 Validation Strategy	12
4. Expected Outcomes and Limitations	13
5. Project Timeline	14
References	14

Developing a Cybersecurity Risk Assessment Framework for Mitigating Spear-Phishing Attacks Against Airline Employees

1. Introduction

1.1 Context and Background

The aviation industry has experienced rapid digital transformation over the past decade. Airlines increasingly rely on interconnected digital technologies to support critical business and operational processes, including reservation systems, employee management platforms, maintenance systems, cloud services, communication networks, and passenger information systems [3], [4]. While these technologies improve efficiency and service delivery, they also increase exposure to cybersecurity threats [13], [14].

Cybersecurity has become a significant concern for aviation organisations due to the growing number of attacks targeting critical infrastructure [1], [3]. Cybercriminals continuously develop new methods to exploit vulnerabilities in organisational systems and human behaviour [16], [21]. Among these threats, phishing attacks remain one of the most common and successful cyberattack techniques [6], [19].

Spear-phishing is a specialised form of phishing in which attackers target specific individuals or groups using personalised information [5], [8]. Unlike traditional phishing campaigns that target large numbers of individuals simultaneously, spear-phishing attacks are carefully crafted to deceive selected victims. Attackers often use publicly available information and social engineering techniques to increase the authenticity of the communication [5], [10], [20].

Airline employees are particularly attractive targets because they often possess privileged access to operational systems, administrative applications, and sensitive passenger information [3], [4]. A successful spear-phishing attack may result in credential theft, data breaches, ransomware infections, and operational disruption [6], [7], [17]. Consequently, there is an increasing need for effective risk management approaches that address both technical and human-related vulnerabilities [1], [2].

1.2 Research Problem

Despite significant investments in cybersecurity technologies, many airlines continue to experience cyber incidents initiated through social engineering attacks [15], [16], [19]. Existing cybersecurity strategies often focus primarily on technical controls such as firewalls, intrusion detection systems, and endpoint protection technologies [1], [2]. Although these controls are important, they are often insufficient against sophisticated spear-phishing attacks that exploit human behaviour [5], [9], [22].

A major challenge within the aviation sector is the absence of a dedicated cybersecurity risk assessment framework specifically designed to analyse and mitigate spear-phishing risks targeting airline employees. Existing frameworks such as the NIST Risk Management Framework and ISO/IEC 27005 provide general risk management guidance but are not specifically tailored to the operational environment of airlines [1], [2]. The aviation industry faces multiple cybersecurity threats capable of

disrupting operations and compromising sensitive information. Understanding the broader threat landscape helps contextualise the significance of spear-phishing attacks.

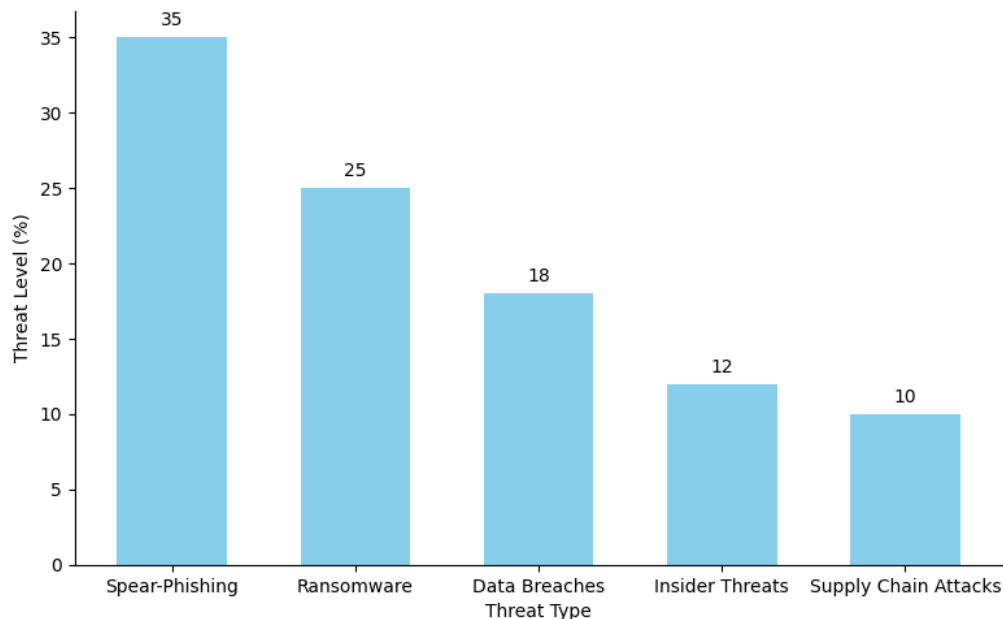


Figure 1. Aviation Cybersecurity Threat Landscape

Figure 1 highlights the principal cyber threats currently affecting aviation organisations, demonstrating the importance of addressing employee-focused attack vectors. The lack of an aviation-specific risk assessment approach limits the ability of security managers to identify, evaluate, and prioritise threats associated with spear-phishing campaigns. This creates a gap between strategic cybersecurity governance and practical risk mitigation activities [11], [21], [23].

Therefore, there is a need to develop a cybersecurity risk assessment framework capable of helping airlines identify spear-phishing threats, assess vulnerabilities, evaluate risks, and implement effective mitigation strategies [1], [2], [21].

1.3 Research Aim and Objectives

Research Aim

To develop a cybersecurity risk assessment framework for mitigating spear-phishing attacks against airline employees.

Research Objectives

1. To identify the common spear-phishing techniques used against airline employees.
2. To examine the organisational, technological, and human vulnerabilities associated with successful spear-phishing attacks.
3. To evaluate spear-phishing risks using established cybersecurity risk assessment principles.
4. To develop an aviation-specific cybersecurity risk assessment framework.
5. To validate the usefulness of the proposed framework using airline cybersecurity case studies.

1.4 Significance of the Research

This research is significant because cyber threats continue to evolve and pose substantial risks to airline organisations [14], [16], [21]. By focusing specifically on spear-phishing attacks against employees, this study addresses an increasingly important cyber risk within the aviation industry [3], [4], [8].

Academically, the research contributes to the growing body of knowledge on aviation cybersecurity by integrating cyber risk assessment concepts with social engineering threat analysis [5], [10], [21].

Practically, the proposed framework may assist cybersecurity professionals and airline management teams in developing more effective risk management practices. The framework could support employee awareness programmes, security policy development, risk prioritisation activities, and incident response planning [1], [2], [22].

From a societal perspective, improved cybersecurity within airlines may contribute to the protection of passenger information, organisational assets, and critical transportation services [3], [4], [7].

2. Literature Review

2.1 Introduction

The purpose of this literature review is to examine existing research relating to aviation cybersecurity, spear-phishing attacks, human factors in cybersecurity, and cybersecurity risk assessment frameworks [1], [2], [3]. The review aims to identify major trends, research gaps, and opportunities for future investigation within the aviation sector, particularly regarding the risks posed by spear-phishing attacks against airline employees [3], [4], [21].

2.2 Aviation Cybersecurity

The aviation industry relies heavily on information and communication technologies. Digital systems support functions such as flight planning, maintenance operations, passenger service management, logistics coordination, and air traffic communication [3], [4]. As dependency on digital infrastructure increases, cyber threats become more significant, creating new security challenges for airlines and other aviation stakeholders [14], [16].

Researchers have identified aviation as part of the critical infrastructure sector due to its importance to economic stability, public safety, and international transport systems [3], [21]. Consequently, cybersecurity incidents affecting airlines may have widespread consequences beyond individual organisations, potentially disrupting transportation networks and exposing sensitive passenger information [4], [7]. Modern airline operations depend on a highly interconnected technological ecosystem consisting of several digital environments.

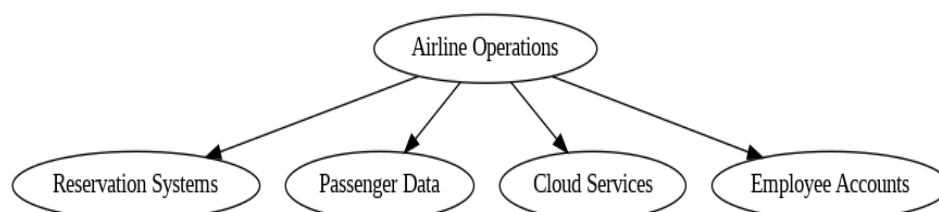


Figure 2. Aviation Cybersecurity Ecosystem

Figure 2 illustrates the interconnected nature of aviation systems and highlights potential entry points available to attackers. Numerous studies indicate that aviation organisations face challenges related to system complexity, legacy technologies, supply-chain dependencies, and increasing connectivity [21], [24]. These factors collectively increase the attack surface available to cyber attackers and create difficulties in maintaining effective cybersecurity controls across diverse operational environments [1], [3].

2.3 Spear-Phishing Attacks

Spear-phishing represents one of the most dangerous forms of social engineering [5], [19]. Attackers gather information about targeted individuals from social media platforms, corporate websites, professional networking sites, and publicly available sources in order to create personalised and convincing attack campaigns [7], [20].

Using this information, attackers create convincing messages designed to encourage recipients to open malicious attachments, click harmful links, or disclose confidential information [8], [10]. Unlike conventional phishing attacks, spear-phishing campaigns are often highly tailored to their targets, increasing the likelihood of successful compromise [5], [17]. Spear-phishing attacks generally follow a predictable sequence that gradually leads to organisational compromise.

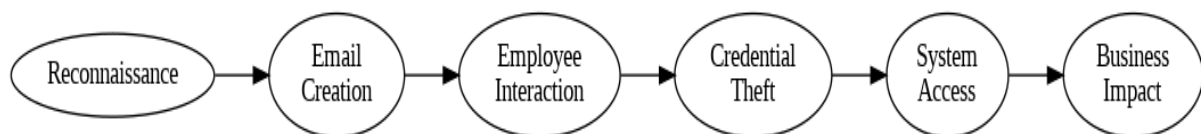


Figure 3. Spear-Phishing Attack Lifecycle Targeting Airline Employees

Figure 3 illustrates the progression of a typical spear-phishing attack from initial reconnaissance to organisational impact, highlighting multiple stages where security controls and employee awareness measures can be applied to reduce risk. Research consistently demonstrates that spear-phishing remains one of the leading causes of credential compromise and unauthorised system access [6], [19]. The personalised nature of these attacks significantly increases their effectiveness compared to traditional phishing campaigns, making them a major concern for organisations operating within critical infrastructure sectors such as aviation [5], [8].

2.4 Human Factors in Cybersecurity

Human behaviour is widely recognised as one of the most important dimensions of cybersecurity [9], [22]. Even organisations that invest heavily in technical security measures remain vulnerable if employees fail to recognise malicious communications or follow secure cybersecurity practices [10], [15].

Several factors influence employee susceptibility to spear-phishing, including lack of awareness, excessive workload, cognitive bias, trust relationships, and insufficient cybersecurity training [5], [9],

[22]. Attackers frequently exploit human psychology rather than technical vulnerabilities, making employee-focused attacks particularly difficult to prevent through technological controls alone [8], [20]. Human behaviour remains one of the most significant factors influencing cybersecurity outcomes within organisations. Understanding the primary factors contributing to employee vulnerability is therefore essential.

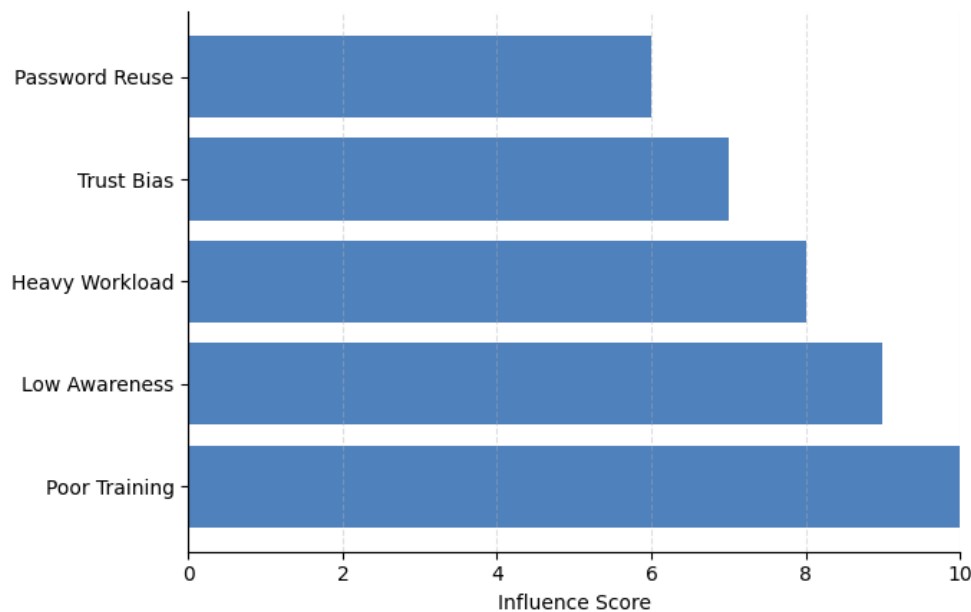


Figure 4. Human Factors Affecting Spear-Phishing Susceptibility

Figure 4 identifies the principal behavioural and organisational factors that may increase employee vulnerability to spear-phishing attacks. Previous studies suggest that cybersecurity awareness programmes can improve employee resistance to phishing attacks [9], [22]. However, awareness training alone may not eliminate all risks. Effective risk management requires a combination of technology, policy, organisational culture, and continuous employee education to strengthen organisational cybersecurity resilience [1], [2], [15].

2.5 Cybersecurity Risk Assessment Frameworks

Cybersecurity risk assessment frameworks provide structured approaches for identifying and managing cyber threats [1], [2]. These frameworks assist organisations in evaluating potential threats, identifying vulnerabilities, assessing risks, and implementing suitable controls to reduce cybersecurity exposure [11], [21].

The NIST Risk Management Framework is widely used to identify risks, assess controls, monitor security performance, and support cybersecurity decision-making processes [1]. Similarly, ISO/IEC 27005 offers internationally recognised guidance for information security risk management and supports organisations in systematically managing cybersecurity risks [2].

In addition to NIST and ISO standards, the OCTAVE framework provides an organisational approach to risk identification, analysis, and mitigation planning [11]. These frameworks have been successfully applied across numerous sectors and provide valuable guidance for cybersecurity governance and risk management [1], [2], [11].

Although these frameworks provide valuable guidance, they are designed for general organisational environments rather than airline-specific cybersecurity challenges [1], [2]. Consequently, there is an opportunity to develop a framework that incorporates both established risk assessment principles and aviation-specific operational requirements, particularly those relating to employee-focused spear-phishing risks [3], [21].

2.6 Research Gap

The literature demonstrates extensive research on aviation cybersecurity and phishing attacks independently. However, relatively few studies focus specifically on spear-phishing threats affecting airline employees from a risk assessment perspective.

Most existing research either addresses technical cybersecurity controls or employee awareness programmes separately. There is limited evidence of frameworks integrating threat identification, vulnerability analysis, risk evaluation, and mitigation planning specifically for airline employees.

This gap provides the foundation for the proposed research.

3. Research Design and Methodology

3.1 Introduction

This chapter describes the research design, methodological approach, data collection procedures, data analysis techniques, research materials, and ethical considerations adopted in this study. The primary aim of this research is to develop a cybersecurity risk assessment framework for mitigating spear-phishing attacks against airline employees. As the study seeks to address a practical cybersecurity challenge while proposing a solution that can be applied within real-world airline environments, a structured and systematic methodology is required to ensure the reliability, validity, and applicability of the research findings [1], [2].

The methodology has been designed to achieve the research objectives through a combination of literature review, risk analysis, and case study evaluation. The study does not involve software development, penetration testing, or access to operational airline systems. Instead, it relies on secondary data sources, established cybersecurity standards, and recognised risk assessment practices to develop and evaluate the proposed framework [1], [2], [21].

3.2 Research Philosophy

This research adopts a pragmatist philosophy. Pragmatism is particularly suitable for studies that aim to solve practical problems and generate actionable outcomes rather than solely contributing to

theoretical knowledge [12]. Since the primary objective of this study is to develop a framework that can assist airline organisations in mitigating spear-phishing risks, a pragmatist perspective provides the flexibility required to focus on practical effectiveness and real-world applicability.

Pragmatism also supports the use of different methods and sources of evidence where appropriate. In this study, both qualitative and quantitative techniques are incorporated to provide a comprehensive understanding of spear-phishing threats, associated vulnerabilities, and mitigation approaches. The philosophy is therefore aligned with the needs of cybersecurity research, where organisational decision-making often depends on balancing theoretical understanding with practical implementation requirements [1], [12].

3.3 Research Approach

A deductive research approach will be employed in this study. The deductive approach begins with existing theories, concepts, and frameworks and applies them to a specific problem domain in order to develop and evaluate solutions [12]. This approach is appropriate because extensive research already exists concerning cybersecurity risk management, social engineering threats, phishing attacks, and information security governance.

The study will draw upon established cybersecurity frameworks such as the NIST Risk Management Framework and ISO/IEC 27005 to examine spear-phishing threats within airline environments [1], [2]. Rather than developing entirely new theoretical concepts, the research seeks to adapt and integrate existing cybersecurity knowledge into a framework specifically focused on mitigating spear-phishing risks against airline employees. The research follows a systematic process from problem identification to framework validation to ensure that the proposed solution is both theoretically grounded and practically applicable.



Figure 5. Research Onion for the Proposed Study

The deductive approach supports the systematic examination of current literature, enabling the researcher to identify recognised risk factors, evaluate existing mitigation techniques, and construct a framework grounded in established cybersecurity best practices [1], [2], [23].

3.4 Research Design

This study adopts a Design Science Research (DSR) methodology.

Design Science Research focuses on creating innovative artefacts designed to solve identified problems. In the context of this research, the artefact is the proposed cybersecurity risk assessment framework for mitigating spear-phishing attacks against airline employees.

DSR is appropriate because the research aims not only to understand the cybersecurity problem but also to provide a practical solution. Unlike purely descriptive research methods, Design Science Research encourages the development, refinement, and evaluation of solutions that can be applied in professional practice.

The research process will be structured into four phases:

Phase 1: Problem Identification

The first phase involves identifying the cybersecurity challenges associated with spear-phishing attacks targeting airline employees. Existing literature, industry reports, and aviation cybersecurity studies will be reviewed to understand the nature and impact of the problem.

Phase 2: Risk Analysis

The second phase focuses on analysing vulnerabilities, threats, and consequences associated with spear-phishing attacks. Risks will be evaluated according to their likelihood and potential impact on airline operations.

Phase 3: Framework Development

The third phase involves designing the cybersecurity risk assessment framework. The framework will incorporate risk identification procedures, vulnerability assessment processes, risk evaluation criteria, and mitigation recommendations.

Phase 4: Framework Evaluation

The final phase focuses on evaluating the usefulness of the framework through selected airline cybersecurity case studies. The framework will be applied to real-world scenarios to assess its effectiveness and practicality.

3.5 Research Method

The study employs a mixed-methods research strategy, combining qualitative and quantitative techniques to address the research objectives [12]. The integration of multiple methods enables a broader understanding of the research problem and improves the overall robustness of the findings.

The qualitative component of the research consists of a detailed literature review, document analysis, industry report analysis, and case study examination. These methods will be used to identify common spear-phishing techniques, employee-related vulnerabilities, security awareness challenges, and current mitigation strategies. Through thematic analysis, key patterns and relationships within the collected information will be identified and interpreted.

The quantitative component incorporates cybersecurity risk assessment techniques commonly applied within information security management. Likelihood and impact ratings will be used to evaluate identified risks, while risk scoring and prioritisation methods will support the classification of security threats according to their severity. By combining qualitative insights with quantitative evaluation, the research aims to develop a comprehensive framework that reflects both theoretical and practical dimensions of cybersecurity risk management [1], [2].

3.6 Data Collection

This research primarily relies on secondary data sources. Secondary data provides access to a broad range of cybersecurity knowledge while avoiding the security, privacy, and ethical concerns associated with collecting sensitive operational data from airlines [1], [21].

Data will be collected from peer-reviewed academic journals, conference proceedings, cybersecurity industry reports, aviation security publications, government reports, NIST publications, ISO standards, and publicly documented airline cyber incidents [1], [2], [3], [4]. These sources have been selected because they provide authoritative, reliable, and up-to-date information relating to cybersecurity threats and risk management practices.

The literature review will focus primarily on research published between 2020 and 2026 to ensure that the study reflects contemporary cybersecurity challenges. Additionally, selected aviation cybersecurity case studies will be analysed to investigate real-world examples of spear-phishing attacks and evaluate how the proposed framework could support risk identification and mitigation activities.

3.7 Data Analysis

The collected data will be analysed using thematic analysis and risk matrix analysis.

Thematic analysis will be applied to qualitative information obtained from academic literature, case studies, and industry reports. This process involves reviewing relevant materials, identifying recurring themes, categorising findings into meaningful groups, and interpreting relationships between key concepts [12]. The technique will support the identification of common spear-phishing techniques, organisational vulnerabilities, human-related risk factors, and effective mitigation practices.

In addition, risk matrix analysis will be employed to assess cybersecurity risks associated with spear-phishing attacks. This approach evaluates risks according to their likelihood of occurrence and potential impact on airline operations. Risk levels will be calculated using the relationship:

$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

The risk matrix enables threats to be prioritised according to their severity, providing a structured basis for selecting appropriate mitigation controls [1], [2], [11]. This analytical process directly supports the development of the proposed cybersecurity risk assessment framework.

3.8 Framework Development Process

The proposed framework will be developed using findings generated through the literature review, case study analysis, and risk assessment activities. The framework incorporates five key components that collectively support the identification, evaluation, and mitigation of spear-phishing risks affecting airline employees.

The first component focuses on threat identification, where common spear-phishing attack techniques such as credential harvesting, business email compromise, malware delivery, and executive impersonation attacks will be analysed [5], [8]. The second component involves vulnerability assessment, examining factors such as insufficient training, weak password practices, limited cybersecurity awareness, and excessive access privileges that may increase employee susceptibility to attacks [9], [22].

The third component centres on risk assessment, where identified threats and vulnerabilities are evaluated using likelihood and impact criteria. Following this stage, appropriate mitigation measures such as multi-factor authentication, employee awareness programmes, email filtering technologies, access control mechanisms, and monitoring solutions will be recommended [1], [2]. Finally, the framework incorporates continuous monitoring and periodic review processes to ensure long-term effectiveness in responding to evolving cyber threats.

3.9 Validation Strategy

The proposed framework will be evaluated using a case study validation approach. Validation is an essential stage within Design Science Research because it provides evidence regarding the usefulness, practicality, and applicability of the developed artefact [12].

Several documented cybersecurity incidents affecting aviation organisations will be examined. The framework will be applied retrospectively to determine whether identified risks could have been recognised and mitigated through the proposed assessment process. The evaluation will focus on criteria such as completeness, practicality, usability, applicability to airline environments, and coverage of identified spear-phishing risks [21].

The validation process will provide an indication of how effectively the framework supports cybersecurity decision-making and contributes to organisational risk management within the aviation sector.

3.10 Research Materials

The resource requirements for this study are relatively modest because the research relies primarily on secondary data analysis rather than experimental implementation. Software tools required for the study include Microsoft Word for documentation, Microsoft Excel for risk analysis and data organisation, and reference management software such as Zotero or Mendeley for citation management. NVivo may also be used to facilitate thematic analysis if required.

Hardware requirements consist of a standard laptop or desktop computer with internet connectivity and access to university library databases. No specialist laboratory facilities, cloud computing

resources, or advanced programming environments are required because the study focuses on framework development rather than software engineering or technical system testing.

3.11 Ethical Considerations

The study will comply with all applicable university research ethics requirements. Since the research relies primarily on publicly available secondary sources, the overall level of ethical risk is considered low.

Nevertheless, several ethical principles will guide the research process. All published materials will be appropriately referenced to ensure compliance with copyright and academic integrity requirements. Any expert feedback obtained during the validation phase will be collected with informed consent, and participant anonymity will be protected where appropriate. Furthermore, all research activities will comply with relevant data protection regulations and institutional ethical guidelines [12].

No confidential airline information, personal employee data, or sensitive operational data will be collected or analysed during the course of the research.

3.12 Chapter Summary

This chapter has described the methodology adopted for the study. A pragmatist philosophy, deductive approach, and Design Science Research methodology have been selected to support the development of a cybersecurity risk assessment framework for mitigating spear-phishing attacks against airline employees [1], [2], [12]. The study employs a mixed-methods strategy, combining qualitative thematic analysis with quantitative risk assessment techniques. Secondary data obtained from academic literature, industry reports, cybersecurity frameworks, and aviation case studies will be used to inform framework development and evaluation. Consequently, the proposed methodology provides a structured, practical, and achievable approach that aligns closely with the research aim and objectives. [1], [2], [21]

4. Expected Outcomes

The research is expected to produce:

- A detailed analysis of spear-phishing threats affecting airline employees.
- Identification of critical employee-related vulnerabilities.
- An aviation-specific cybersecurity risk assessment framework.
- Recommended mitigation strategies for airline organisations.

The proposed framework may support improved cybersecurity governance, employee awareness, and risk management within airlines.

Limitations

Potential limitations include:

- Reliance on publicly available incident data.
- Limited access to internal airline security information.
- Potential challenges in obtaining expert feedback.
- Variations in cybersecurity practices across different airlines.

5. Project Timeline

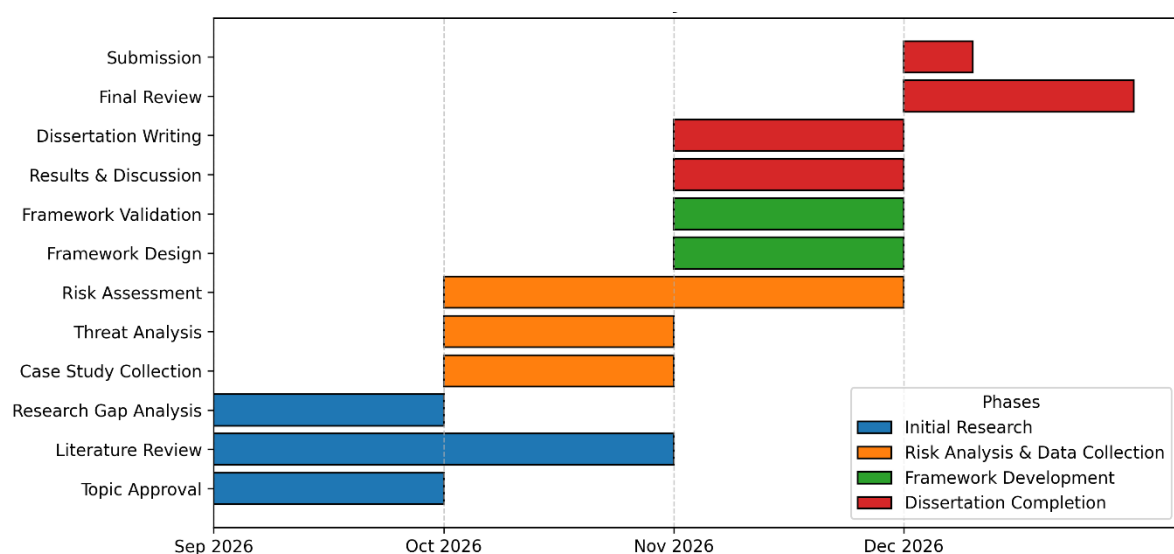


Figure 6. Project Timeline

Figure 6 illustrates the planned sequence of project activities, showing that the primary research tasks are expected to be completed by November 2026, with December reserved for final revisions and submission.

References

- [1] National Institute of Standards and Technology (NIST), *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST Special Publication 800-37 Rev. 2, Gaithersburg, MD, USA, 2024.
- [2] International Organization for Standardization (ISO), *ISO/IEC 27005: Information Security, Cybersecurity and Privacy Protection - Guidance on Managing Information Security Risks*, Geneva, Switzerland: ISO, 2022.

- [3] International Civil Aviation Organization (ICAO), *ICAO Cybersecurity Strategy*, Montreal, Canada: ICAO Publications, 2024.
- [4] International Air Transport Association (IATA), *Aviation Cyber Security Toolkit*, Montreal, Canada: IATA Publications, 2024.
- [5] S. Albladi and G. Weir, "User Characteristics That Influence Judgment of Social Engineering Attacks," *Human-Centric Computing and Information Sciences*, vol. 10, no. 1, pp. 1-24, 2023.
- [6] Verizon, *2025 Data Breach Investigations Report*, New York, NY, USA: Verizon Enterprise Solutions, 2025.
- [7] IBM Security, *Cost of a Data Breach Report 2025*, Armonk, NY, USA: IBM Corporation, 2025.
- [8] European Union Agency for Cybersecurity (ENISA), *Threat Landscape for Social Engineering Attacks*, Athens, Greece: ENISA, 2024.
- [9] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson and C. Jerram, "The Human Aspects of Information Security Questionnaire (HAIS-Q)," *Computers & Security*, vol. 42, pp. 165-176, 2022.
- [10] R. Heartfield and G. Loukas, "Detecting Semantic Social Engineering Attacks Using Natural Language Processing," *Computers & Security*, vol. 93, 2023.
- [11] C. Alberts and A. Dorofee, *OCTAVE Allegro: Improving the Information Security Risk Assessment Process*, Pittsburgh, PA, USA: Software Engineering Institute, Carnegie Mellon University, 2021.
- [12] M. Saunders, P. Lewis and A. Thornhill, *Research Methods for Business Students*, 9th ed., Harlow, United Kingdom: Pearson Education, 2023.
- [13] Cisco Systems, *Cisco Cybersecurity Readiness Index 2025*, San Jose, CA, USA: Cisco Systems, 2025.
- [14] World Economic Forum, *Global Cybersecurity Outlook 2025*, Geneva, Switzerland: World Economic Forum, 2025.
- [15] ISACA, *State of Cybersecurity Report 2024*, Schaumburg, IL, USA: ISACA, 2024.
- [16] Microsoft, *Microsoft Digital Defense Report 2025*, Redmond, WA, USA: Microsoft Corporation, 2025.
- [17] CrowdStrike, *Global Threat Report 2025*, Austin, TX, USA: CrowdStrike, 2025.
- [18] Check Point Research, *Annual Cyber Security Report 2025*, Tel Aviv, Israel: Check Point Software Technologies, 2025.
- [19] J. Hong, "The State of Phishing Attacks," *Communications of the ACM*, vol. 55, no. 1, pp. 74-81, 2022.
- [20] A. Ferreira and S. Teles, "Persuasion: How Phishing Emails Influence Users and Bypass Security Awareness," *International Journal of Human-Computer Studies*, vol. 125, pp. 19-31, 2022.
- [21] M. Alazab and S. Venkatraman, "Cybersecurity Threats and Mitigation in Critical Infrastructures," *Journal of Network and Computer Applications*, vol. 213, pp. 103-125, 2024.

- [22] S. Furnell and K. Thomson, "Recognising and Addressing Human Aspects of Information Security," *Information Management & Computer Security*, vol. 27, no. 1, pp. 5-17, 2022.
- [23] A. Shostack, *Threat Modeling: Designing for Security*, 2nd ed., Indianapolis, IN, USA: Wiley, 2023.
- [24] European Union Agency for Cybersecurity (ENISA), *Cybersecurity Skills Development in the Transport Sector*, Athens, Greece: ENISA, 2024.