A DEEP DIVE INTO EMPLOYEE CYBERSECURITY AWARENESS IN PHARMACY REGULATORY BODY

GAN KANG YAN

PROJECT REPORT SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF CYBER SECURITY

FACULTY OF INFORMATION SCIENCE AND TECHNOLOGY
UNIVERSITY KEBANGSAAN MALAYSIA
BANGI
2024

PENELITIAN MENDALAM TENTANG KESEDARAN KESELAMATAN SIBER PEKERJA DALAM BADAN PENGAWAL FARMASI

GAN KANG YAN

PROJEK YANG DIKEMUKAKAN UNTUK MEMENUHI SEBAHAGIAN
DARIPADA SYARAT MEMPEROLEH IJAZAH
SARJANA K`ESELAMATAN SIBER

FAKULTI TECHNOLOGI DAN SAINS MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2024

DECLARATION

I hereby declare that the work in this project report is my own except for quotations and summaries which have been duly acknowledged.

27 May 2024

GAN KANG YAN
P118152

ACKNOWLEDGEMENT

I extend my deepest gratitude to my supervisor, Prof. Madya Dr. Khairul Akram Bin Zainol Ariffin, whose guidance, expertise, and unwavering support have been instrumental in shaping this thesis. His insightful feedback and constructive criticism have immensely contributed to the quality and depth of the research.

I express sincere appreciation to the pharmacy regulatory body (ABC), the study site for this research. The cooperation and valuable insights provided by the organization greatly enriched the study, allowing for a comprehensive exploration of information security awareness within its context.

Financial support is acknowledged with heartfelt thanks to the Public Service Department (JPA) under the "Hadiah Latihan Persekutuan (HLP)." This support has significantly eased the challenges associated with undertaking this research and is deeply appreciated.

I extend my gratitude to the five subject matter experts whose involvement in validating and weighting the focus areas added a layer of expertise to the research process. Their contributions have been invaluable in ensuring the robustness and validity of the study.

A special mention goes to my former colleagues at ABC, whose support and cooperation were crucial in the successful execution of this research. Their willingness to share insights and experiences added depth to the study, and I am grateful for their collaborative spirit.

To all individuals and organizations who, in various capacities, contributed to the realization of this thesis, I offer my sincere thanks. Your support has been a driving force, and I am truly appreciative of the collective efforts that have shaped this research endeavor.

ABSTRAK

Aktiviti digital yang meluas akibat pandemik COVID-19 yang berpanjangan telah mengubah dinamik tempat kerja, dengan model kerja hibrid menjadi semakin biasa digunakan di kebanyakan organisasi. Transisi ke arah tempat kerja yang lebih fleksibel ini, yang disertai dengan desakan yang berterusan untuk meningkatkan fleksibiliti dalam bekerja dari jarak jauh, telah memperluas bidang serangan siber. Ini menuntut pelaburan strategik dalam penyelesaian keselamatan siber yang khusus dan disasarkan untuk menangani ancaman baharu ini. Walaupun bergantung secara meluas kepada langkah-langkah keselamatan yang berpandukan teknologi, insiden keselamatan maklumat masih berlaku. Ini menyerlahkan peranan penting faktor manusia dan proses dalam memastikan keberkesanan langkah-langkah keselamatan. Terutamanya, sektor penjagaan kesihatan menyaksikan peningkatan kes insiden siber sepanjang tempoh pandemik COVID-19. Pelbagai kajian menekankan faktor manusia sebagai elemen paling lemah dalam rangka kerja keselamatan siber. Oleh itu, kajian ini bertujuan untuk meneroka, menilai dan menangani tahap kesedaran keselamatan maklumat dalam kalangan warga sesebuah organisasi (ABC). Untuk makluman, penyelidikan ini telah menerima kelulusan etika daripada Jawatankuasa Penyelidikan Perubatan dan Etika (MREC) mengikut Panduan Amalan Klinikal yang Baik Malaysia. Penyerahan terperinci kepada NMRR dan MREC mencerminkan langkah-langkah berketat yang telah diambil untuk melindungi kerahsiaan dan integriti data penyelidikan. Antara objektif kajian ini termasuklah mengenal pasti bidang tumpuan yang mempengaruhi keselamatan maklumat, menilai tahap kesedaran dalam kalangan, mengenalpasti bidang-bidang khusus untuk penambahbaikan. Pengesahan soal selidik pula melibatkan penilaian pakar dan Proses Hierarki Analitik (AHP). Proses analisis data melibatkan penggunaan Pearson Product Moment, Alpha Cronbach, analisis statistik deskriptif, dan Ujian Kruskal-Wallis. Soal selidik yang dicadangkan terdiri daripada tiga dimensi dan sembilan fokus utama yang diselaraskan dengan keperluan organisasi bagi menilai tahap kesedaran siber para pekerja. Sembilan fokus utama yang ditentukan ialah "pengurusan kata laluan", "penggunaan emel", "penggunaan internet", "rangkaian sosial", "pelaporan insiden", "penggunaan peranti mudah alih", "pengendalian maklumat", "latihan" dan “polisi”. Keputusan kajian mendedahkan sebuah soal selidik khusus untuk mengukur tahap kesedaran keselamatan siber para pekerja, dengan tahap kesedaran keseluruhan bagi ABC pada 79.15%, dikategorikan sebagai “sederhana”. Secara keseluruhannya, hasil kajian ini menyumbang kepada aspek keselamatan maklumat dalam sektor penjagaan kesihatan dengan mengemukakan cadangan intervensi hasil daripada analisis mendalam terhadap landskap kesedaran siber sedia ada di ABC. Soal selidik yang dibangunkan diharap dapat menjadi panduan berguna kepada organisasi lain dalam memperkukuhkan aspek keselamatan siber masing-masing selaras dengan Strategi Keselamatan Siber Malaysia 2020-2024 yang memberi penekanan kepada tadbir urus berkesan, pembangunan kapasiti, dan peningkatan kesedaran keselamatan siber. Peranan sektor kesihatan sebagai Infrastruktur Maklumat Kritikal Negara menyerlahkan keperluan kawalan keselamatan siber yang kukuh, selaras dengan Dasar Keselamatan Siber Negara yang diperkenalkan pada tahun 2006.

ABSTRACT

The pervasive digital activities triggered by the prolonged COVID-19 pandemic have reshaped work dynamics, with hybrid models becoming prevalent across organizations. This transition, coupled with a continued emphasis on remote work flexibility, has expanded the attack surface, demanding targeted investments in specialized security solutions. Despite extensive reliance on technology-driven security measures, security incidents persist, underscoring the overlooked role of people and processes. Notably, the healthcare sector has witnessed a surge in cyber incidents, especially during the COVID-19 pandemic. Numerous studies underscore the human factor as the most vulnerable link in the security framework. This research aims to explore, assess, and address information security awareness within the healthcare organization (ABC), contextualized within the broader Malaysian information security landscape. Notably, this research has received ethical approval from the Medical Research and Ethics Committee (MREC) in accordance with Malaysian Guidelines for Good Clinical Practice. The detailed submissions to NMRR and MREC highlight the rigorous measures in place to safeguard the confidentiality and integrity of research data. The objectives of this study are to explore the focus areas that significantly impact information security awareness within the pharmacy regulatory body in the public sector, assess the level of information security awareness within the pharmacy regulatory body, and identify the strengths and weakness of information security awareness within the pharmacy regulatory body. The research methodology encompasses a thorough literature review, adaptation of the Human Aspects of Information Security Questionnaire (HAIS-Q) and identifying the focus area. Then validation involves expert evaluation and the Analytic Hierarchy Process (AHP). The data analysis process involves Pearson Product Moment, Cronbach's alpha, descriptive statistical analysis, and the Kruskal-Wallis Test. The innovative questionnaire comprises three dimensions, Knowledge, Attitude and Behaviour, and nine focus areas, aligning with organizational conditions to gauge employee cyber awareness. The nine focus areas are "password management," "email use," "internet use," "social media use," "incident reporting," "mobile device use," "information handling," "training," and "policy." The study's results reveal a nuanced method for measuring employee information security awareness, with an overall awareness level for ABC at 79.15%, categorized as "monitor" or average. The research significantly contributes to healthcare information security, offering actionable recommendations derived from a thorough analysis of ABC's information security awareness landscape. Rooted in the Malaysian regulatory context, the developed questionnaire serves as a valuable resource for organizations seeking to fortify their information security posture. Recommendations align with the Malaysia Cyber Security Strategy 2020-2024, focusing on effective governance, capacity building, and cybersecurity awareness. The healthcare sector's designation as a Critical National Information Infrastructure (CNII) underscores the need for robust cybersecurity controls, as mandated by the National Cyber Security Policy (NCSP) formulated in 2006.

TABLE OF CONTENT

LIST OF TABLES

LIST OF ILLUSTRATIONS

LIST OF ABBREVIATIONS

ABC	Study Site of This Research
AHP	Analytic Hierarchy Process
DKICT	Dasar Keselamatan ICT (ICT Security Policy)
ENISA	European Union Agency for Network and Information Security
HAIS-Q	Human Aspect Information Security-Questionnaire
KAB	Knowledge, Attitude, Behavior
MAMPU	Modernization of Administration and Management Planning Unit of Malaysia
SMEs	Subject Matter Experts

CHAPTER I

INTRODUCTION

1.1 RESEARCH BACKGROUND

The healthcare industry has become a primary target for cyberattacks, making it the most preferred industry for malicious actors. Cybercriminals are increasingly focusing their efforts on exploiting vulnerabilities in healthcare applications that collect and consolidate patient data into Electronic Health Records (EHRs) (Alharam & El-Madany 2018). EHRs serve as comprehensive repositories of electronic health information, containing crucial data such as demographics, medical history, medication details, laboratory test results, and billing information (Jalali et al. 2019). Healthcare applications and systems in the healthcare industry are characterized by their critical nature and dynamic environment. As a result, traditional security mechanisms alone are inadequate to protect against the sophisticated threats they face (Kruse et al. 2017). While some traditional security measures may be adapted and employed, healthcare industries require strong and tailored security approaches to safeguard their systems from cyberattacks and protect patient data.

The South-Eastern Norway Regional Health Authority (South-East RHF), responsible for healthcare services in south-eastern Norway, experienced a major security breach in January 2018(Irwin 2018). The breach compromised the protected health information (PHI) and records of approximately 2.9 million individuals, accounting for over half of Norway's population. The attack is believed to have been orchestrated by a sophisticated criminal group, potentially linked to a foreign spy or state agency. The organization's legacy system, Windows XP, served as the vulnerability that was exploited (Khandelwal 2018). Despite security measures being planned, the attack occurred before their implementation. This breach raised concerns

regarding future motivated attacks targeting healthcare data and highlighted compliance issues with the General Data Protection Regulation (GDPR) (Ashford 2018). Unfortunately, the affected individuals were not notified within the required 72-hour timeframe. This incident underscores the urgent necessity for robust information security measures in the healthcare sector and emphasizes the importance of adhering to data protection regulations.

In recent years, the COVID-19 pandemic has accelerated the digital transformation across various sectors, including the healthcare industry (OECD 2020). The rapid adoption of cloud technologies, increased reliance on digital platforms, and the generation of vast amounts of sensitive data have revolutionized healthcare operations. However, this digitization has also exposed vulnerabilities and gaps in cybersecurity defenses, posing significant risks to patient privacy and data security.

Although the threat of COVID-19 may be diminishing, the heightened digital activity spurred by the pandemic continues unabated. Hybrid work models have become increasingly popular and are likely to become standard practice for many organizations. Even as employees return to physical offices, the expectation of remote work flexibility persists. This dynamic expands the attack surface that enterprises must safeguard, necessitating focused investments in specialized security solutions.

In the first half of 2022, ransomware attacks witnessed a staggering year-over-year growth of nearly 52% (Dessai 2022). Notably, ransomware-as-a-service attacks orchestrated by well-known hacking organizations like Conti and LockBit, which caused significant disruptions during the height of the pandemic, experienced a 500% YoY surge (Dessai 2022). These statistics underscore the persistent and evolving threat landscape that organizations face.

Both governmental entities and private corporations have integrated technology into their operations, connecting crucial assets to the internet to enhance services and maintain a competitive edge(Alkhazi et al. 2022). To safeguard their information infrastructure and data, both government agencies and private firms have intensified their focus on technology-driven security measures. However, this emphasis on

technology alone overlooks the integral role of people and processes in achieving effective security (Pattinson et al. 2018) Consequently, even organizations with substantial investments in robust security technologies continue to experience security incidents(Abzakh & Althunibat 2023; Mäses 2015; Neigel et al. 2020).

Numerous studies have highlighted the human factor as the most vulnerable link in the security framework (Abzakh & Althunibat 2023; Broberg & Sinnott n.d.; Neigel et al. 2020; Shah et al. 2023; Yeo et al. 2023). Both organizations and researchers have recognized the gravity of this threat, leading to the development of various strategies to mitigate the associated risks (Broberg & Sinnott n.d.; Shah et al. 2023; Yeo et al. 2023). In a general sense, there are four main approaches to risk management: avoiding risk, transferring risk, retaining risk, and reducing risk (Mäses 2015).Several research efforts have proposed that awareness assessment and training represent the most efficacious approach to thwarting these attacks, emphasizing that human constitute the last line of defense against various cyber risks (Alkhazi et al. 2022; Pattinson et al. 2020; Rajamaki et al. 2018). As a result, organizations should not rely exclusively on technological remedies; instead, they should proactively tackle human vulnerabilities and allocate resources towards enhancing awareness of information security.

Within the context of the ABC (study site), regulatory staffs play a crucial role in ensuring the safety and efficacy of medications. As custodians of valuable patient information and sensitive pharmaceutical data, they are increasingly targeted by cybercriminals seeking to exploit vulnerabilities in healthcare systems. The evolving threat landscape, coupled with the potential consequences of a successful cyber-attack, necessitates a comprehensive understanding of information security awareness among employees.

The results of this study will offer valuable perspectives into the current state of information security awareness among employees in the study site, which will be referred to as "ABC" in our subsequent research, helping to identify areas for improvement and inform the development of tailored interventions. Ultimately, the goal is to empower employees with the knowledge and skills necessary to protect data,

counter potential cyber threats and safeguard the integrity of pharmaceutical regulatory processes.

By addressing the specific context of ABC, this research aims to make a significant contribution to the field of healthcare information security. The outcomes of this study will not only benefit the ABC and regulatory staff but also have broader implications for public sector seeking to enhance information security awareness and resilience in the face of increasing cyber threats.

1.2 PROBLEM STATEMENT

The human factor becomes pivotal, and research emphasizes the significance of prioritizing information security awareness among employees (Abzakh & Althunibat 2023). In the specific context of the ABC, regulatory staff, critical custodians of healthcare data, may lack adequate knowledge regarding information security threats and best practices (Yeng et al. 2022). This knowledge gap poses a substantial risk, as unaware behaviors could compromise data security or make them susceptible to cyberattacks(Yeng et al. 2022; Yeo et al. 2023). Various factors, including attitudes towards risks and vulnerabilities, awareness of the organization's policies, and training in the proper use of countermeasures, influence employees' information security behaviors. In the realm of information security (Yeo et al. 2023), significant emphasis is placed on the human factor, often referred to as the "first line of defense" against threats (Von Solms & Van Niekerk 2013). In recent empirical investigations, an exploration of factors affecting information security awareness (ISA) among employees in conventional work environments has been conducted. Different personal characteristics, such as age, gender, education, personality traits, propensity for risk-taking, preferred learning styles, and habits related to internet usage, have been identified as factors associated with the levels of information security awareness among employees. The significant financial consequences of cyber-attacks underscore the crucial importance of information security, as evidenced by a 2019 study commissioned by Microsoft. According to the findings, healthcare organizations in the Asia Pacific region could incur an average cost of US$ 23.3 million. (Gnaneswaran 2019). Within the context of this research, the information security landscape at ABC concerning

threats and best practices heightens associated risks. This prompts an exploration into dimensions such as knowledge, attitudes, and behaviors regarding risks, along with an awareness of organizational policies and training in countermeasure usage. In-depth examinations of human factors influencing information security awareness have extensively utilized the HAIS-Q, focusing on essential areas such as “password management”, “e-mail use”, “internet use”, “social media use”, “incident reporting”, “mobile devices use” and “information handling” in employees' daily work practices.

While technical measures are integral, relying solely on them is insufficient, as evidenced by cyber incidents in Malaysia predominantly related to fraud. Researchers, such as Parsons, McCormac, Butavicius, et al. (2014), emphasize that prioritizing the information security of employees is crucial. According to Cybersecurity Malaysia, the highest reported cyber incidents in 2023 in Malaysia were related to fraud, with a total of 2,078 cases. Between 2017 and 2021, Assistant Director of Telecommunications Criminal Investigation at the Bukit Aman Commercial Crime Investigation Department (CCID), Supt Rozeni Ismail, disclosed that the country documented an astonishing 98,607 instances of online fraud, resulting in significant financial losses amounting to RM3.3 billion (Ministry of Communications and Digital n.d.). For instance, the World Health Organization (WHO) and its partners have experienced a significant increase in hacking attempts through phishing websites during COVID-19 pandemic (He et al. 2021). In response to this growing threat, the WHO issued a warning to the public, urging them to exercise caution (World Health Organization n.d.). The ABC plays a pivotal role in safeguarding the nation's public health through the regulation and supervision of pharmaceutical products and medical devices. In an increasingly digital and interconnected healthcare landscape, information security has emerged as a pressing concern to protect sensitive healthcare data and preserve the integrity of healthcare systems. However, this concern is further underscored by recent findings, including the Cisco Cybersecurity Readiness Index, which revealed that merely 16% of organizations in Malaysia exhibit a 'mature' level of readiness to confront modern cybersecurity risks (Cisco Secure 2023). The Index, sourced from a double-blind survey of 6,700 private sector cybersecurity leaders spanning 27 territories across North America, Latin America, EMEA, and Asia-Pacific, highlights the urgency of cybersecurity readiness. Additionally, an overwhelming 95% of respondents foresee a

cybersecurity incident disrupting their business in the next 12 to 24 months. Considering this challenging landscape, the research seeks to investigate the current level of information security awareness among regulatory staff within the ABC. Cyber threats, highlighted by the significant increase in cyber incidents related to fraud, underscore the importance of evaluating the proficiency of the organization in responding to modern cybersecurity risks. The study seeks to comprehend the existing knowledge among regulatory staff concerning information threats, best practices, and potential risks associated with their daily activities.

With cyber-attacks posing a significant financial risk to healthcare organizations in the public sector, prioritizing and fortifying the information security of employees becomes imperative. According to a scoping review conducted by He et al. (2021), the healthcare sector faces substantial information security challenges, encompassing aspects such as ensuring remote work security, mitigating human errors, addressing insufficient security awareness, managing budget constraints, and addressing vulnerabilities in current systems. By delving into the current cybersecurity landscape and evaluating the maturity level of organizations in Malaysia, the study aims to identify both strengths and weaknesses in information security awareness within the pharmacy regulatory body in the public sector. The strengths and weaknesses in information security awareness within the pharmacy regulatory body remain unidentified, hindering the development of targeted improvement initiatives. This identification of strengths will offer valuable insights into areas that can be leveraged to enhance the overall information security posture of the organization, contributing to the preservation of sensitive healthcare data and the integrity of healthcare systems in Malaysia.

In conclusion, the research aims to explore the specific focus areas of information security awareness relevant to the research context. Subsequently, it will assess the current level of information security awareness among regulatory staff within the ABC. The next step involves identifying the strengths and weaknesses of information security awareness in the pharmacy regulatory body within the public sector. By addressing these challenges, the research endeavors to enhance information security awareness, effectively safeguarding pharmaceutical and healthcare data and preserving the integrity of public health in Malaysia.

1.3 RESEARCH QUESTION

Based on the problem statement, there are several research questions that have been identified, namely:

1. What are the focus areas need to be included in assessing the information security awareness within pharmacy regulatory body in the public sector?
2. What is the extent of information security awareness among staff within the pharmacy regulatory body in the public sector, specifically focusing on the identified key areas?
3. What are the strengths of information security within the pharmacy regulatory body in the public sector?

1.4 OBJECTIVE

1. To explore the focus areas that significantly impact information security awareness within the pharmacy regulatory body in the public sector.
2. To assess the current level of information security awareness among staff within the pharmacy regulatory body in accordance with the identified focus areas
3. To identify the strength of the information security awareness within pharmacy regulatory body in the public sector.

1.5 RESEARCH SCOPE

The scope of works for this information security awareness assessment within ABC encompasses a comprehensive examination of knowledge, attitudes, and behaviors related to information security among the staff. The assessment will include the administration of the HAIS-Q questionnaire to a defined target population within ABC, covering various departments and job roles. In adherence to national research standards, we initiate the research registration process through the National Medical Research Register (NMRR) platform. This registration is imperative as our study involves Ministry of Health (MOH) facilities and personnel. Additionally, recognizing the ethical considerations inherent in research, we diligently seek approval from the

Medical Research and Ethics Committee (MREC) in accordance with the Malaysian Guidelines for Good Clinical Practice. Emphasizing the importance in protecting sensitive data and participant privacy, our submission to NMRR and MREC provide detailed information on the robust measures implemented to ensure the confidentiality and integrity of research data. Through this dual process of NMRR registration and ethical approval, our research endeavors to contribute responsibly to the understanding and enhancement of information security practices in our specific context. The survey will be conducted over a specified timeframe to capture a snapshot of information security awareness. Data collection will be carried out through an online survey platform, ensuring confidentiality and ethical considerations. The scope also involves identifying specific focus areas within pharmacy regulatory body in public sector where information security is relatively weaker and requires improvement. This encompasses evaluating the level of information security awareness and ultimately offering recommendations based on strengths and weaknesses.

1.6 THESIS STRUCTURE

This thesis unfolds across five pivotal chapters, each serving a distinct purpose. Chapter I, the Introduction, provides a concise overview of information security incidents and awareness, elucidating the problem statement, objectives, and the study's scope. Chapter II, the Literature Review, navigates through information security and cybersecurity, exploring the human aspect, analytic hierarchy process, and pertinent theories and frameworks like the Knowledge, Attitudes, and Behaviors (KAB) Model and the Human Aspects of Information Security Questionnaire (HAIS-Q). Transitioning to Chapter III, we meticulously detail the study's methodology, employing a questionnaire as an instrument to assess information security readiness. This encompasses processes such as revising the HAIS-Q, validating the questionnaire, and implementing the Analytic Hierarchy Process. We also delve into the intricacies of data collection and analysis. Chapter IV is dedicated to the analysis and elucidation of findings derived from the questionnaire, including the result of validity and reliability test, result of information security awareness level, and a comprehensive discussion of test outcomes, along with presentation and interpretation. The focus area in this study include: “password management”, “e-mail use”, “internet use”, “social media use”,

"incident reporting", "mobile devices use", "information handling", "training" and "policy". Finally, Chapter V synthesizes the overarching conclusions drawn from the study, encapsulating limitations, and proposing avenues for future research.

CHAPTER II

LITERATURE REVIEW

2.1 INTRODUCTION

The literature review serves as a foundational exploration conducted prior to the study, enhancing our comprehension of the research context, and providing a detailed elaboration. This chapter encompasses several key elements, beginning with an examination of information security and cybersecurity. In our study, the emphasis is on information security, as we intend to assess both the physical and cyberspace information security of staff members. A significant portion of this review is dedicated to the human aspect within information security. This entails a comprehensive exploration of human factors influencing cyber incidents and information security, shedding light on the intricate relationship between individuals and the security of information systems. The chapter further delves into relevant theories and frameworks, including the Knowledge, Attitudes, and Behaviors Model, as well as the HAIS-Q. These theoretical foundations play a pivotal role in shaping our understanding of the human dimension in information security. Additionally, the literature review encompasses an investigation into the acceptance of HAIS-Q, involving a synthesis of previous studies that have utilized or incorporated the HAIS-Q framework. By consolidating this information, we aim to build a robust knowledge base that informs our subsequent discussions and analyses in this thesis. In essence, this comprehensive literature review sets the stage for an in-depth exploration of human factors within information security, providing a nuanced understanding of key concepts and theoretical underpinnings crucial to the overarching objectives of our research.

2.2 INFORMATION SECURITY AND CYBERSECURITY

“Information security” and “cyber security” are frequently used interchangeably, although there exists a nuanced distinction between the two. Von Solms & Van Niekerk (2013) argue that while information security primarily revolves around safeguarding data in terms of “availability”, “integrity”, and “confidentiality”, cyber security extends beyond this scope (Abzakh & Althunibat 2023; Von Solms & Van Niekerk 2013). Cyber security encompasses not only the protection of information but also the safeguarding of individuals, societal values, and national infrastructure. It addresses the broader spectrum of interests, including both information and non-information-based assets, that require protection from the risks associated with their interactions in cyberspace(Reid & van Niekerk 2014). Importantly, humans and their societies are integral components of the assets in need of protection. Cyberspace is defined as a “complex environment resulting from the interaction of people, software, and services on the Internet through technology devices and connected networks, which lacks a physical from”(Reid & van Niekerk 2014) . Recognizing this, many security experts and nations emphasize the imperative for public awareness and education to enhance cybersecurity.

Information security, as defined by the SANS Institute (SANS n.d.), encompasses "processes and methodologies designed and implemented to safeguard print, electronic, or any other form of confidential, private, and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption." It is noteworthy that the mention of "print" emphasizes the protection of information or data in various formats, not exclusively digital or electronic. In contrast, cybersecurity, as articulated by technology leader Cisco(Cisco n.d.), involves "the practice of protecting systems, networks, and programs from digital attacks." These attacks typically target sensitive information with the intent of accessing, altering, or destroying it, extorting money from users, or disrupting normal business processes.

Therefore, while cybersecurity and information security are closely intertwined and share some commonalities, their primary distinction lies in their focus on information. Information security is dedicated to safeguarding information across all

mediums, whereas cybersecurity specifically targets information in cyberspace. Illustratively, consider a scenario where sensitive information is left on an employee's desk and is copied by a customer with the intention of selling it to an unauthorized party (Taherdoost 2022). This constitutes a breach in information security as cyberspace is not involved in the process. However, if the same sensitive information is shared on social media by the employee, damaging the company's reputation, it is deemed a breach in both cybersecurity and information security.

In the context of this research, the term "information security" is employed. The term is utilized to cover a spectrum of factors associated with safeguarding information in various dimensions, including both online environments (cyberspace) and physical realms. It includes considerations not only related to technical measures but also non-technical aspects, recognizing that information security involves a holistic approach that extends to the physical handling, storage, and protection of sensitive information, not solely confined to digital platforms. This broad perspective allows for a more inclusive exploration of factors affecting information security across diverse contexts and domains.

2.3 THE HUMAN ASPECT OF INFORMATION SECURITY

In systems involving human interaction, individual actions play a significant role (Hadlington 2018a). This complex interplay of human and systems introduces the potential for security breaches stemming from both inadvertent human errors and deliberate malicious activities, such as the use of weak passwords, accessing harmful websites, or sharing information with unauthorized parties (Abzakh & Althunibat 2023; Shah et al. 2023). Referred to as "insider threats," employees within organizations may engage in actions with malicious intent, whether consciously or unintentionally (Yeo et al. 2023). Often, individuals may lack awareness of the malicious implications of their behavior, and in some cases, they may simply disregard potential consequences.

Shouran et al. (2019), in their exploration of "Information System Security: Human Aspects," highlight five crucial human factors that significantly impact information security. These factors encompass the “lack of motivation”, “lack of awareness”, “risky beliefs”, “behavior”, and the “inadequate use of

technology”(Shouran et al. 2019), shedding light on the multifaceted aspects of human behavior in the realm of information security.

Hadlington et al. (2019) highlight the dual role of employees as a crucial asset in preventing cyberattacks and, simultaneously, as individuals who are inclined to "just get the job done," leading to occasional mistakes. Hadlington (2018a) emphasis on the impact of deficiencies in skills, knowledge, and awareness is corroborated by participants' responses, revealing significant gaps in information security competencies. A substantial portion of respondents, constituting 58%, expressed a lack of knowledge or skills pertaining to dealing with information security incidents. Moreover, 55% indicated that they did not feel adequately equipped with the necessary skills to safeguard the company against cybercrime. Next, the findings underscore issues related to insufficient attention to information and awareness concerning key risks, with a notable 84% of participants feeling that there is already an ample amount of information available about communicating key risks related to cybercrime. Moreover, a lack of adherence to security practices may stem from the misconception that relying solely on technical security measures is sufficient protection against cyberattacks. When users fail to adopt secure behaviors, the human factor emerges as a threat to information security solutions (Hadlington 2018b). Consequently, behaviors characterized by missteps, lack of awareness, or a careless approach can jeopardize the information security of an entire organization.

Human beings are often the weakest link in cyber ecosystem, and it is essential for health facilities to prioritize raising awareness among all users(Argaw et al. 2020). Although it cannot guarantee absolute security, prioritizing information security awareness is a positive step forward. In healthcare settings, diverse personnel such as clinicians, billing professionals, as well as patients and caregivers linking personal devices to the hospital network, may unintentionally or deliberately present cybersecurity risks. The potential for human error, as illustrated by the occurrence at Geneva University Hospital (HUG) in October 2019, further underscores the introduction of vulnerabilities (Ganten et al. 2018). To mitigate these risks, recommendations from the European Union Agency for Network and Information Security (ENISA)'s “Security and Resilience in eHealth” publication and others

emphasize the importance of providing cybersecurity awareness and training (Kruse et al. 2017). For instance, it is important for individuals to possess knowledge about the potential risks to privacy and data integrity that arise when storing data on mobile devices. Furthermore, the utilization of connected or removable devices amplifies the potential for malware execution, heightening the risk level. End users should also have a strong understanding of various threats, including ransomware attacks, their effects, and how they are initiated.

The World Health Organization (WHO) and its partners have experienced a significant increase in cyber-attack attempts through phishing websites (He et al. 2021). In response to this growing threat, the WHO issued a warning to the public, urging them to exercise caution (World Health Organization n.d.). One notable incident involved hacker orchestrating an attack on the WHO by creating a malicious website that impersonated an email login portal for WHO employees(Al-Qahtani & Cresci 2022). The objective of this attack was to steal passwords from unsuspecting employees. Although the WHO has stated that the attack was not successful, it serves as a stark reminder that phishing attacks can be used to target health organizations(Al-Qahtani & Cresci 2022). This incident highlights the need for increased awareness and vigilance regarding phishing attacks, particularly within the healthcare sector.

The cyberattack on the European Medicines Agency (EMA) has resulted in the unauthorized access and leakage of documents related to COVID-19 medicines and vaccines (EMA 2021). The leaked documents included internal emails dated back to November, which pertained to the evaluation processes for COVID-19 vaccines. Some of the leaked correspondence has been manipulated by the attackers, potentially undermining trust in vaccines.

According to a scoping review conducted by He et al. (2021), the healthcare sector encounters substantial information security challenges. These challenges encompass various aspects such as ensuring remote work security, mitigating human errors, addressing insufficient security awareness, conducting thorough risk assessments, addressing gaps in business continuity planning, establishing coordinated incident response protocols, managing budget constraints, and addressing

vulnerabilities in medical systems. The challenges, intensified by the COVID-19 pandemic, emphasize the critical imperative for healthcare organizations to prioritize information security awareness. By recognizing these challenges and promoting awareness, healthcare organizations can take proactive steps to prevent cyber threats and protect sensitive patient data.

A bibliometric analysis conducted by Jalali et al. in 2019 examined the literature on information security in healthcare over the past two decades. Their analysis covered 472 English-language journal articles. The findings revealed that more than half of the studies focused on technological and management aspects of information security (Jalali et al. 2019). However, the analysis also highlighted a potential research gap, suggesting that literature may have relatively overlooked human and organizational aspects, along with physical security, in the healthcare domain.

ENISA conducted a study that identified security expertise and awareness as significant challenges in eHealth cybersecurity(Liveri et al. 2015). This is a critical concern since minimizing human errors, which can contribute to successful cyberattacks, is paramount. The study highlighted that the human factor is considered the primary cause of security failures in certain countries, such as Austria. Addressing these challenges and improving security expertise and awareness are crucial in mitigating cybersecurity risks in the eHealth sector.

Human play a pivotal role in information security as even well-trained IT staff alone is not sufficient to mitigate all threats. Many information security incidents stem from human error or a lack of awareness (Rajamaki et al. 2018). In the context of eHealth systems, user credentials can be compromised through social engineering techniques, even in robustly secured environments. Risk awareness is crucial in guiding users' decision-making processes when encountering cyber threats. User compliance with information security rules relies on their knowledge and understanding of these rules(Ceesay et al. 2018). Therefore, promoting user awareness and ensuring their comprehension of cybersecurity measures are essential for effective cyber risk management.

Table 1.1 Summaries of past information security incidents in healthcare organizations

Organizations	Reported Details	Type of Attack	Impacts
South-East RHF (Norway) (Irwin 2018)	Major information security breach compromising PHI of 2.9 million individuals	Sophisticated criminal attack, potentially politically motivated	Compromised protected health information, raised compliance issues with GDPR, underscored need for robust information security measures in healthcare
World Health Organization (WHO) (Al-Qahtani & Cresci 2022)	Hacking attempts through phishing websites	Phishing	Increased risk of stolen passwords, need for heightened awareness and vigilance regarding phishing attacks
US Department of Health and Human Services (HHS) (Stein & Jacobs 2020)	Distributed Denial of Service (DDoS) attack	DDoS	Attempted disruption of pandemic response efforts
European Medicines Agency (EMA) (EMA 2021)	Unauthorized access and leakage of documents related to COVID-19 medicines and vaccines	Data breach, potentially manipulated correspondence	Undermined trust in vaccines, compromised sensitive information

2.4 THEORIES AND FRAMEWORKS.

2.4.1 Knowledge, Attitudes and Behaviors Model

The fundamental principle of the Knowledge, Attitude, and Behavior (KAB) model is to comprehend the connection between its three components. It suggests that as individuals acquire knowledge, it influences their attitudes and ultimately their behaviors. In the domain of information security, knowledge signifies employees' understanding of information security concepts, attitude reflects their perceptions and sentiments toward information security, and behavior denotes the actions they undertake in relation to security risks. According to the KAB model, an increase in employees' knowledge of security behaviors corresponds to an enhancement in their attitudes, consequently leading to improved information security-related behaviors.

Kruger and Kearney (2006) introduced a prototype that offers a measurement framework for evaluating ISA. The study specifically examines the ISA of employees within an international mining company. The framework comprises three core components, each translated into corresponding dimensions:

1. Knowledge (“relating to what is known”)
2. Attitude (“concerning what is perceived”)
3. Behavior (“in relation to what is done”).

These dimensions form the basis for gauging and comprehending the extent of ISA among employees in the company. (Kruger & Kearney 2006).

Kruger and Kearney (2006) categorized their study into six risk categories, which they also referred to as "Golden rules":

1. “Always adhere to company policies.”
2. “Keep passwords and personal identification numbers (PINs) secret.”
3. “Use e-mail and the Internet with care.”
4. “Be careful when using mobile equipment.”
5. “Report incidents like viruses, thefts and losses”
6. “Be aware, all actions carry consequences.”

A set of thirty-five questions was formulated to assess the knowledge, attitude, and behavior of respondents concerning the six focus areas which was outlined in the previously discussed "six golden rules, along with their respective factors and sub-factors as depicted in figure 2.1. To enhance specificity, and through consensus, the six focus areas were subdivided into more detailed factors. For instance, the focus area of passwords was disaggregated into two subcategories: “purpose of passwords” and “confidentiality of passwords”. Further granularity within the confidentiality of passwords category was achieved by breaking it down into two sub-factors: “writing down of passwords” and “giving passwords to others” (Kruger & Kearney 2006).

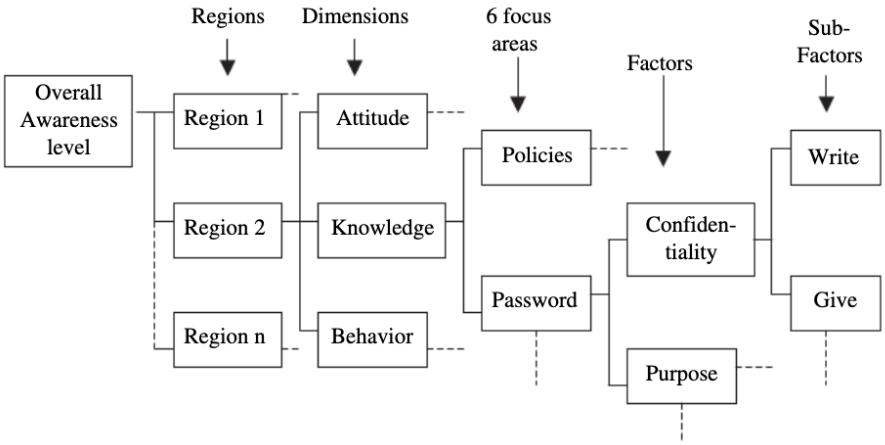

Figure 2.1 Tree structure of Kruger & Kearney Knowledge, Attitudes and Behaviours Model

Source: Kruger & Kearney 2006

2.4.2 Human Aspects of Information Security Questionnaire (HAIS-Q)

The HAIS-Q focuses on three dimensions: Knowledge, Attitude, and Behavior (KAB), aimed at evaluating information security within a workplace. These aspects are segmented into multiple ISA focus areas, facilitating a thorough evaluation of an organization's information security status (Parsons et al. 2017; Parsons, McCormac, Butavicius, et al. 2014; Parsons, McCormac, Pattinson, et al. 2014). Through the assessment of knowledge, attitudes, and behaviors, HAIS-Q provides insights into the effectiveness of an organization's information security practices and identifies areas for improvement.

Parsons et al. (2014) examined multiple information security policies and, through interviews with senior management, identified seven focus areas, as documented in subsequent works:

1. “Password management”
2. “E-mail use”
3. “Internet use”
4. “Social networking site use”
5. “Incident reporting”

6. “Mobile computing”

7. “Information handling”

In comparison to the study conducted by Kruger & Kearney (2006), the seven focus areas identified by Parsons et al. (2014) are more granular and specific. Moreover, this study explicitly outlines three representative sub-areas for each focus area.

The HAIS-Q, created by Parsons and collaborators, serves as a valuable instrument for assessing individuals' ISA (Parsons, McCormac, Butavicius, et al., 2014). Aligned with the KAB model, this measurement tool posits that as an employee's knowledge of ISA, their attitude will enhance, leading to enhance information security behaviors (Kruger & Kearney 2006; Parsons, McCormac, Butavicius, et al. 2014). The development of the HAIS-Q involved a comprehensive review of information security policies and standards, coupled with consultations with managers and information technology professionals. Through this meticulous process, Parsons and colleagues identified seven focus areas for their measurement tool.(Parsons, McCormac, Butavicius, et al. 2014) (see Figure 2.2).

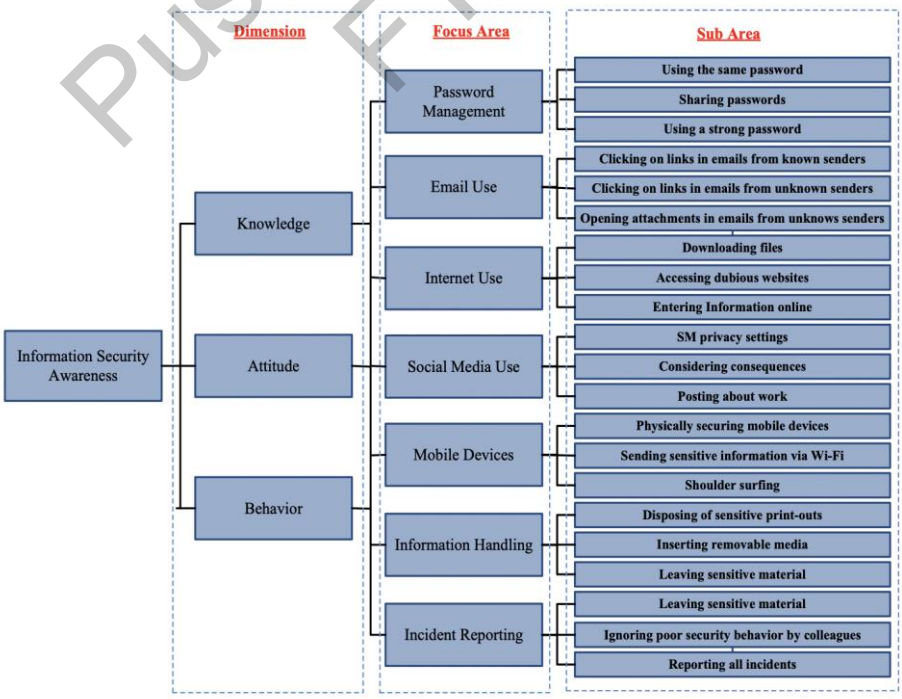

Figure 2.2 Three dimensions and the focus area of HAIS-Q model

Source: Parsons, McCormac, Butavicius, et al. 2014

The HAIS-Q, tailored for assessing employee KAB in relation to information security, offers management a benchmark for evaluating the efficacy of diverse IT control strategies. It also facilitates continuous monitoring of the organization's long-term security health.

Based on senior management interviews and existing literature emphasizing the role of human errors in information security breaches, the study by Parsons et. al. (2014) sets forth the following hypotheses:

"H1: Better knowledge of policy and procedures is associated with a more positive attitude towards policy and procedures."

"H2: A more positive attitude towards policy and procedures is associated with self-reported behavior that is more risk averse."

"H3: Better knowledge of policy and procedures is associated with self-reported behavior that is more risk averse."

Through these hypotheses, the study (Parsons, McCormac, Butavicius, et al. 2014) aims to explore the interconnectedness between KAB concerning policy and procedures in the context of using work on computers.

Parsons and colleagues have dedicated efforts to precisely conceptualize knowledge, ensuring specificity and alignment of the KAB statements within the sub-areas of HAIS-Q. In contrast to similar measures such as the UNISAQ, the HAIS-Q has undergone comprehensive testing for both reliability and validity (Parsons et al. 2015, 2016, 2017; Parsons, McCormac, Butavicius, et al. 2014; Parsons, McCormac, Pattinson, et al. 2014).

To assess validity, the HAIS-Q underwent a three-phase process. Initially, an expert in survey design reviewed the questionnaire in the first phase to ensure accurate phrasing and prevent misunderstandings in the questions. Subsequently, a pilot was carried out involving working Australians in the second phase (Parsons, McCormac, Pattinson, et al. 2014). Following this, Cronbach's alpha was employed to gauge the internal consistency of the survey. In the third phase, the survey was administered to

500 working Australians, and similarly, Cronbach's alpha was utilized for internal consistency, evaluated separately for each focus area, as in the previous phase (Parsons, McCormac, Butavicius, et al. 2014; Parsons, McCormac, Pattinson, et al. 2014). The findings corroborated the theory that heightened knowledge corresponds to enhanced attitudes and improved security behavior (Parsons, McCormac, Pattinson, et al. 2014)

To further validate the reliability of the HAIS-Q, additional studies were conducted by Parsons et al. (2017). In the initial study, university students underwent a phishing test without their knowledge, and the results were compared with their HAIS-Q scores. The outcomes indicated that students with higher HAIS-Q scores performed better in the phishing test, supporting convergent validity. The second study involved 505 working Australians participating in the survey, where all 63 items of the HAIS-Q were examined, providing additional support for construct validity. Additionally, the study demonstrated the HAIS-Q's capacity to pinpoint ISA needs within specific focus areas (Parsons et al. 2017)

2.5 APPLICATION OF HAIS-Q IN MEASURING THE INFORMATION SECURITY AWARENESS

The human aspects frequently assume a more pivotal role in attaining holistic information security (Abzakh & Althunibat 2023; Ceesay et al. 2018). Individuals utilizing information technology exhibit variations in their KAB regarding information security. The HAIS-Q is designed to gauge information security performance, considering the KAB of users across seven focus areas, as mentioned earlier.

The HAIS-Q has gained widespread acceptance in scientific and professional circles, being employed in various research. For example, individuals scoring higher on the HAIS-Q exhibited superior performance in a phishing experiment, suggesting its potential as a reliable predictor of information security behavior (Parsons et al. 2017) Additionally, research has indicated that several factors assessed by the HAIS-Q are linked to enhanced practices in cyber hygiene (Neigel et al. 2020). Furthermore, in the study conducted by Wiley et al. (2020), the HAIS-Q revealed gender differences (Wiley et al. 2020). This study also underscores the significance of organizational and security cultures, highlighting that improvements in these areas are crucial alongside ISA.

According to the findings, an enhancement in an organization's culture will positively influence its security (Wiley et al. 2020). As a result, the HAIS-Q stands out as a cutting-edge questionnaire for evaluating the information security performance of individuals.

Recent applications of the HAIS-Q extend across various domains of information security, including the evaluation of information security practices among hospital staff (Fauzi et al. 2021) and the formulation of methodologies for assessing ISA (Vilander 2021). The HAIS-Q holds significance both in theoretical and practical contexts. From a theoretical standpoint, extensive utilization across diverse populations (Parsons et al. 2016), such as students, the general public, and personnel from government and financial sectors, has been instrumental in its reliability and validity in various contexts, making it a valuable instrument for research purposes.

Zulfia et al. (2019) conducted a study at a corporate (PT. PQS) to evaluate awareness, specifically focusing on the impact of human error on information security breaches. The study employed the HAIS-Q to assess vulnerability to threats arising from employee behavior. The obtained Cronbach's Alpha coefficients, ranging from .790 to .932, indicate that the HAIS-Q is a dependable measurement instrument for assessing employees' information security awareness in the context of PT. PQS (Zulfia et al. 2019).

Furthermore, a separate study conducted by Candara and Ruldeviyani (2019) examined the effectiveness of the HAIS-Q within the context of XYZ firm. In this study, Cindana utilized Kruger's scale to measure ISA, categorizing scores into three levels: scores of 80-100 were classified as "Good," scores of 60-79.99 were considered average and in need of improvement, and scores of 0-59.99 were categorized as poor and requiring immediate action. The study findings indicated that the overall score for the ISA measurement was 87.59, reflecting a classification of "Good." (Cindana & Ruldeviyani 2019).

In their publication, Parsons et al. (2014) discuss the influence of various factors, such as demographics and organizational culture, on KAB dimensions. This observation is supported by subsequent investigations (McCormac et al. 2017; Tsohou

et al. 2015; Wiley et al. 2020). To enhance the understanding of ISA scores, it is recommended to incorporate questions related to these factors into the questionnaire. This inclusive approach not only aids in the interpretation of ISA scores but also contributes to the customization of ISA programs for specific groups (Takens 2020). The focus areas utilized in past information security studies incorporating HAIS-Q are presented in table 2.1. The details regarding whether the studies used the full version, or a modified version of HAIS-Q are presented in Appendix C. Additionally, the specifics of the modifications made to the questionnaire are also explained.

Table 2.1 Summaries of the focus areas utilized in past information security studies incorporating HAIS-Q are presented.

Research Title	FA 1	FA 2	FA 3	FA 4	FA 5	FA 6	FA 7	FA 8	FA 9	FA 10	FA 11	FA 12	FA 13	FA 14
(Snyman et al. 2017)	/	/	/	/			/		/					
(Pattinson et al. 2018)	/	/	/	/	/	/	/		/					
(Cindana & Ruldeviyani 2019)	/	/	/	/	/	/	/							
(Anon 2019)	/	/	/	/	/	/	/							
(Zulfia et al. 2019)	/	/	/	/	/	/	/							
(Normandia et al. 2019)	/	/	/	/		/	/	/		/				
(Takens 2020)	/	/		/	/		/							
(Nield et al. 2020)	/	/	/	/	/	/	/				/	/		
*(Zimmermann & Renaud 2021)	/	/	/	/	/	/	/							
(Fadhilah et al. 2021)	/	/	/	/	/	/	/							
(Firsty Arisya et al. 2020)	/	/	/	/	/	/	/							
(Prakoso et al. 2020)	/	/	/	/	/	/	/							
(Neigel Et Al. 2020)	/	/	/	/	/	/	/							
(Lee & Ariffin 2021)	/	/	/	/	/	/	/							
(Fujs et al. 2021)	/	/	/	/	/	/	/							
(Hadlington & Chivers 2021)	/	/	/	/			/							
(Vilander 2021)	/	/	/	/	/	/	/							
(Gangire et al. 2021)	/	/	/	/	/	/	/						/	
**(Schmidt et al. 2021)														

to be continued…

…continuation

(Nohlberg 2021)		/	/	/										
(Fauzi et al. 2021)	/	/	/	/		/	/							
(Effendy et al. 2022)	/	/	/	/	/	/	/							
(Rosihan & Hidayanto 2022)	/	/	/	/	/	/	/	/		/				
(Alkhazi et al. 2022)	/	/	/	/	/	/	/		/					
(Hermawan et al. 2022	/	/	/	/	/	/	/							
(Destya Atlanta et al. 2022)	/	/	/	/	/	/	/							
(Fadlika et al. 2023)	/	/	/	/	/	/	/							/
DKICT	/	/	/	/	/	/	/	/	/					
Percentage (%)	93	96	93	96	79	82	93	11	14	7	4	4	4	4

FA1= “Password management”
FA2= “Email Use”
FA3= “Internet Use”
FA4= “Social Media Use”
FA5= “Mobile Device”
FA6= “Information Handling”
FA7= “Incidence Reporting”
FA8= “Policy”
FA9= “Training”
FA10= “Computer Security Work”
FA11= “Data Breach”
FA12= “GDPR”
FA13= “Privacy”
FA14= “ISO/IEC 27001:2013”

* The adapted HAIS-Q only included sections on attitude and behaviour

** The questionnaire was adapted from the HAIS-Q, which condensed its seven dimensions related to computer and data use into three questions: Awareness: “I am aware of external threats against our data and computers”, Attitude: “I find that the IT department’s initiatives to secure data and computers are more of a nuisance than a benefit”, Behavior: “I am attentive towards how I operate computers to avoid being hacked

2.6 IDENTIFYING THE FOCUS AREA

While there are alternative measurement constructs for assessing compliance, only a limited number consider KAB components. The selection of the HAIS-Q was based on its distinct advantages, including robust reliability and validity, a comprehensive array of consistent factors, relevance to contemporary and alignment with organizational policies. One of the key strengths of the HAIS-Q lies in its extensive involvement in various research projects and samples, with over 2,000 working professionals and governmental personnel having participated in the questionnaire across numerous research endeavors.

As mentioned, the HAIS-Q encompasses a total of 63 items, a scale that may be considered expansive, particularly in scenarios where time is a limiting factor (Parsons et al. 2017). Given the independent validation of all focus areas, there exists the flexibility to gauge specific aspects of ISA by selecting one or more pertinent focus areas tailored to the research objective. The modular nature of the HAIS-Q design allows for customization to the researcher's needs, where it is not necessary to incorporate all seven focus areas or three dimensions, although adopting this comprehensive approach would provide the deepest understanding of an individual's (Parsons et al. 2017).

While most studies employ the complete questionnaire without alterations, there are instances where researchers modify the HAIS-Q, such as by creating a shortened version (short-HAIS-Q) (Hadlington & Chivers 2021). Alternatively, researchers have been known to customize the HAIS-Q by either adding or removing specific focus areas (Nield et al. 2020), among other modifications. Additionally, some studies opt to integrate the HAIS-Q with other questionnaires, incorporating them without altering the fundamental composition of the HAIS-Q (Gangire et al. 2021; Hadlington et al. 2020; Wiley et al. 2020; Zimmermann & Renaud 2021).

As an illustration, the examination of Internet-based awareness can be conducted using part of the focus area in HAIS-Q as indicators like email use, internet use, and social media use, as suggested by Nohlberg (2021). Furthermore, researchers have the flexibility to focus on a single component of the model while excluding the

others, as outlined by Parsons et al. (2017). This partial application has been observed, particularly in the banking industry, where it was applied exclusively to the attitude and knowledge dimensions among employees(Pattinson et al. 2016).

Considering the sustainability of the HAIS-Q methodology, it is recommended to incorporate extra focus areas to tackle the changing landscape of threats and advancements in technology (Parsons et al. 2017). The development of a questionnaire for measuring information security awareness entails identifying crucial components, relationships, and factors that play a role in evaluating and enhancing information awareness within an organization.

This research takes into consideration of the element of Information and Communication Technology (ICT) Security Policy (DKICT) (MAMPU 2019) which is implement in the context of ABC. The Prime Minister's Department, through the Modernization of Administration and Management Planning Unit of Malaysia (MAMPU), has issued the DKICT to meet the enforcement requirements, control, and comprehensive measures to protect government ICT assets. All government agencies are responsible for ensuring the implementation and compliance of the Government ICT framework. DKICT is applicable to all users in the Ministry who manage, maintain, process, access, load, provide, upload, share, store, and use ICT assets.

The DKICT is a comprehensive document outlining the information security policy in the Malaysian context. It covers various aspects related to the ICT within organizations. The policy addresses key areas such as risk assessment, organizational safety structures, and the roles of individuals in ensuring ICT security. It also delves into the management of ICT assets, including the categorization and control of information, physical and environmental security measures, and guidelines for human resource security. The DKICT extends its coverage to operational and communication management, emphasizing the importance of secure development and maintenance of information systems. Additionally, it provides directives for incident management, ensuring a systematic approach to handling security incidents. The policy concludes with sections on business continuity management, compliance with legal requirements, and enforcement measures for policy violations. Overall, the DKICT serves as a

comprehensive framework to guide organizations in implementing effective measures to safeguard their ICT infrastructure and information assets.

In the third section of the DKICT KKM, specifically addressing Human Resource Security, it is outlined that Ministry of Health (KKM) is required to undertake several initiatives. Firstly, KKM is mandated to conduct awareness and educational sessions focusing on ICT security management for its users. This emphasizes the importance of imparting knowledge and understanding regarding the principles and practices of information and communication technology security within the organization. Additionally, KKM is directed to provide awareness, training, or education on ICT security at least once a year. This periodic engagement aims to ensure that the personnel associated with KKM stay informed and updated on the evolving landscape of ICT security, reinforcing their capabilities to contribute to a secure and resilient information environment.

To integrate DKICT KKM and HAIS-Q into our questionnaire, we initiated the process by examining the components within the DKICT. A thorough literature review was then conducted to investigate previous studies on information security awareness that incorporated HAIS-Q. The comparison involved scrutinizing the content of HAIS-Q focus areas and identifying key elements within DKICT as shown in Table 2.1. This analysis led us to delve deeper into the training and policy components, considering their significance in both HAIS-Q and DKICT. This comprehensive approach ensures a robust questionnaire that aligns with essential elements from both frameworks.

2.6.1 Research Exploring the Integration of Policy Factors with HAIS-Q

A study carried out by Rosihan & Hidayanto (2022) focused on the Indonesian Correctional Institution and employed the KAMI Index, and the HAIS-Q for assessment. Employing a questionnaire with 87 questions drawn from the HAIS-Q and KAMI Index, the study assessed nine focus areas across KAB dimensions (Rosihan & Hidayanto 2022). Validity testing utilized the Pearson Product Moment method to determine the suitability of each question for assessing the desired outcome. Additionally, reliability testing, employing the Alpha-Cronbach method, gauged the consistency and trustworthiness of the measuring instrument when repeated. The work

introduced a new sub-focus area within password management, emphasizing the significance of securing passwords in the current context where many organizations promote multi-factor authentication. Additionally, a factor of "Information Security Policy" was incorporated as a new focus area to evaluate its importance and the level of adherence among participants.

In a study conducted by Normandia et al. (2019), the inclusion of an Information Security Policy as a new focus group aimed to evaluate both the importance and adherence to the policy. The validity test conducted on each indicator was deemed valid, as the computed correlation coefficient (r count) exceeded the critical value (r table). Additionally, the reliability test results for each variable indicated reliability, as the calculated Alpha-Cronbach coefficient surpassed the threshold of 0.5 (Normandia et al. 2019). These findings suggest that the Information Security Policy in the study is not only valid in its assessment but also exhibits reliability in measuring both importance and adherence.

In the study by Nield et al. (2020), survey instruments were formulated by integrating questions derived from the HAIS-Q. Beyond the established HAIS-Q categories, the researcher introduced three additional focus areas: "data breaches", the "Notifiable Data Breaches scheme (NDB)", and "GDPR awareness" (Nield et al. 2020). For example, the "Notifiable Data Breaches scheme" encompassed subareas like "NDB awareness", "NDB adherence", and "NDB reaction", identified as critical aspects for the research. Questions under each subarea were formulated to gather participant data regarding their awareness of the policy and legislation, compliance with its requirements, and their behavioral reactions to it.

2.6.2 Research Exploring the Integration of Training Factors with HAIS-Q

In the investigation by Snyman et al. (2017), the inquiry was constructed based on the key focus areas and subjects delineated HAIS-Q. Notably, the additional new focus area of security training portraying positive behavior, specifically, volunteering for information security training. This addition served as a control to assess respondents' inclination to emulate others in their behavior when there was no negative association with the conduct.

The paper by Pattinson et al. (2018) pursues a dual objective (Pattinson et al. 2018). Firstly, it introduces a framework of controls focused on the human aspects of information security. Secondly, it empirically assesses the effectiveness of a specific adaptive control—namely, the nature of information security training provided. In addressing the second aim, the study incorporated inquiries about participants' information security training experiences, covering types and frequency of training. Additionally, the Cybersecurity Learning Styles Inventory was utilized to determine individuals' favored approaches to learning about cybersecurity.. The study's results affirm the hypothesis that tailoring training to individuals' learning styles enhances ISA, promoting safer non-malicious behavior when using digital devices for work. Table 2.1 presents summaries of research studies that employed the HAIS-Q, whether in its full version or a modified iteration.

The establishment of initial focus areas in this study involves a fusion of existing research components and the DKICT framework. Through an extensive literature review, nine focus areas were selected for the initial questionnaire, drawing on their identification in previous studies, as outlined in Table 2.1. Table 2.2 presents summaries of the elements present in DKICT and HAIS-Q, accompanied by the justification for selecting each focus area.

Table 2.2 The focus area identified based on literature review.

Focus Area	Details
"Password management"	This focus area is adapted from the HAIS-Q model, assessing practices such as using the same password for personal and work accounts, sharing passwords, and employing strong passwords. With the advent of newer technology, an additional sub-focus area to consider is securing passwords with multi-factor authentication (MFA). This aspect is also extensively addressed in the DKICT KKM, specifically under the category of "User Password Management".
"Email Use"	This focus area is adapted from the HAIS-Q model, specifically focusing on clicking on links in emails from known senders, clicking on links in emails from unknown senders, and opening attachments in emails from unknown senders. In DKICT KKM, the usage of email and related information is discussed in the "Management of Email or Electronic Messages.
"Internet Use"	This focus area is adapted from the HAIS-Q model, covering aspects such as downloading files, accessing dubious websites, and entering information online. The utilization of the internet is addressed in DKICT KKM under the section of "Network Security Management".

to be continued…

… continuation

"Social Media Use"	This focus area is adapted from the HAIS-Q model, addressing social media privacy settings, considering consequences of social media use, and posting about work. The aspect of privacy related to work is regulated under the Official Secrets Act 1972 in DKICT KKM.
"Mobile devices Use"	This focus area is adapted from the HAIS-Q model, encompassing physically securing mobile devices, sending sensitive information via Wi-Fi, and shoulder surfing. This aspect is also extensively addressed in the DKICT KKM, specifically under the category of "Bring Your Own Device".
"Information handling"	This focus area is adapted from the HAIS-Q model, involving disposing of sensitive printouts, inserting removable media, and leaving sensitive material behind. This aspect is also extensively addressed in the DKICT KKM, specifically under the category of "Information Classification and Handling".
"Incident Reporting"	This focus area is adapted from the HAIS-Q model, encompassing reporting suspicious behavior, ignoring poor security behavior by colleagues, and reporting all incidents. This aspect is also extensively addressed in the DKICT KKM, specifically under the category of "Incident Handling Management".
"Policy"	This focus area is derived from the elements in DKICT KKM, addressing awareness and adherence to policy. Further details are provided under "Development and Coordination of Policies" In DKICT KKM. Research that integrates policy factors: (Neild et al. 2020; Normandia et al. 2019; Rosihan & Hidayanto 2022)
"Training"	This focus area is derived from the elements in DKICT KKM, which cover about awareness and importance of training in information security. Further details have been discussed under "Cultivation, Training, and Information Security Awareness Sessions" in DKICT KKM. Research that Integrates Training Factors: (Pattinson et al. 2018; Snyman et al. 2017)

2.7 CONCLUSION

After conducting a thorough examination of the existing literature, this chapter embarks on a comprehensive exploration of key topics essential to our research. The chapter evaluates the context of information security, delves into human factors in information security, and assesses the application of HAIS-Q, drawing insights from previous studies that have incorporated or utilized the questionnaire. Through this extensive literature review, our goal is to establish a nuanced understanding of fundamental concepts and theoretical foundations, laying the groundwork for subsequent discussions and analyses in this thesis. This chapter particularly focuses on the human factors in information security and aims to develop a questionnaire consisting of nine focus areas, including "password management," "email use," "internet use," "social networking," "incident reporting," "mobile device use," "information handling," "training," and "policy."

CHAPTER III

METHODOLOGY

3.1 INTRODUCTION

This chapter outlines the comprehensive research methodology employed in this study, detailing the systematic approach taken to investigate information awareness within the context of the ABC organizations. The methodology comprises a series of sequential steps designed to ensure a rigorous and methodical exploration of the research objectives. The initial phase involves a thorough literature review, which serves as the foundation for understanding relevant research and existing models used in assessing information security awareness. The selection of HAIS-Q is justified based on its established reliability and validity, as discussed earlier. Following this, the questionnaire undergoes meticulous revisions tailored to suit the specific needs of ABC. Next, focus areas are developed incorporating the revised HAIS-Q, DKICT and other relevant research components. Validation is a critical step in the research process, wherein subject matter experts evaluate the questionnaire items for appropriateness and relevance. The Analytic Hierarchy Process (AHP) is then applied to assign weights to the identified focus areas, contributing to an overall assessment of information security awareness. Prior to actual data collection, a pilot study is conducted to refine research instruments and procedures. The subsequent phase involves real data collection, a significant stage where information is systematically gathered for thorough analysis. The data analysis process is geared towards extracting meaningful insights from the collected data. Importantly, the research goes beyond analysis, culminating in the provision of recommendations derived from the research outcomes. To enhance clarity and comprehension, the methodological steps are visually represented in Figure 3.1, providing a clear overview of the research process. This visual aid aims to make the

intricate research methodology more accessible to readers, offering a concise representation of the steps undertaken in this study.

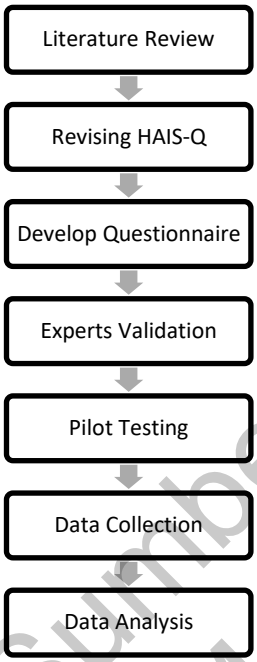

Figure 3.1 Research steps

3.2 LITERATURE STUDY

The research involves a comprehensive literature review, employing search terms such as "cybersecurity," "information security," “information security awareness,” and "HAIS-Q." The objectives of the literature review are multifaceted. Firstly, it aims to gain a deep understanding of information security, exploring its various dimensions. Secondly, the review seeks to comprehend the theories and frameworks that form the foundation for assessing information security awareness, with a specific focus on the HAIS-Q. Additionally, the review aims to identify relevant focus areas applicable to the context of a pharmacy regulatory body within the public sector. Lastly, the literature review serves as a valuable guide in shaping the overall research process, facilitating the conceptualization and execution of the study.

The initial phase of this research involves a literature review aimed at comprehending the information security measurement framework utilized in this study, specifically the HAIS-Q. This exploration seeks to elucidate how the framework contributes to gauging information security awareness within an organization. A

thorough understanding of the significance of information security, the encompassed domain, and diverse instruments for assessing information security levels is crucial. Chapter II provides a detailed account of the definitions of information security and cybersecurity, along with the previous studies which are HAIS-Q related.

This study employs the HAIS-Q framework developed by Parsons et al. (2014). The primary questionnaire comprises seven focus areas that delineate aspects of an information security involving employees and their adherence to it. Each of these areas encompasses three sub-areas, as illustrated in Figure 2.2. The measurement of each sub-area involves three levels of assessment: Knowledge, Attitude, and Behavior (KAB). All seven focus areas from the HAIS-Q are considered important and closely related to the context of ABC, thus they are included in the questionnaire development. Additionally, other factors and areas, such as policy and training, have been thoroughly reviewed and included as new focus areas in the identification of the focus area.

The next step involves identifying the research focus area, with the selection of the HAIS-Q model incorporating the KAB dimensional variable and the seven focus areas. The choice of research focus area is guided by the context of the ABC organization. Notably, the literature review reveals a scarcity of research focused on specific user groups within public organizations in Malaysia, underscoring the necessity to elucidate their differences and add to the current understanding of designing ISA programs.

The outcome of the literature review informs the construction of the questionnaire, incorporating question components derived from the focus areas of the HAIS-Q and integrating elements from the DKICT. The details in Table 2.2. The DKICT was meticulously examined to confirm the inclusion of essential components. Consequently, this study identifies nine key focus areas, namely “password management”, “email usage”, “internet usage”, “social media usage”, “mobile device”, “information handling”, “incident reporting”, “policy” and “training”, as detailed in Table 3.1. The added focus areas include policy and training, with a specific sub-focus on “Password Management” advocating for the implementation of multi-factor authentication to bolster password security (Rosihan & Hidayanto 2022). This

expansion is driven by the literature review, underscoring the critical role of comprehending information security policies, participating in relevant training, and aligning with the guidelines set forth in DKICT KKM. These focus areas serve as the foundational components of the questionnaire, providing a comprehensive framework for assessing information security awareness within the context of the study. The figure 3.2 shows the correlation among the problem statement, objectives, methods, and anticipated outcomes.

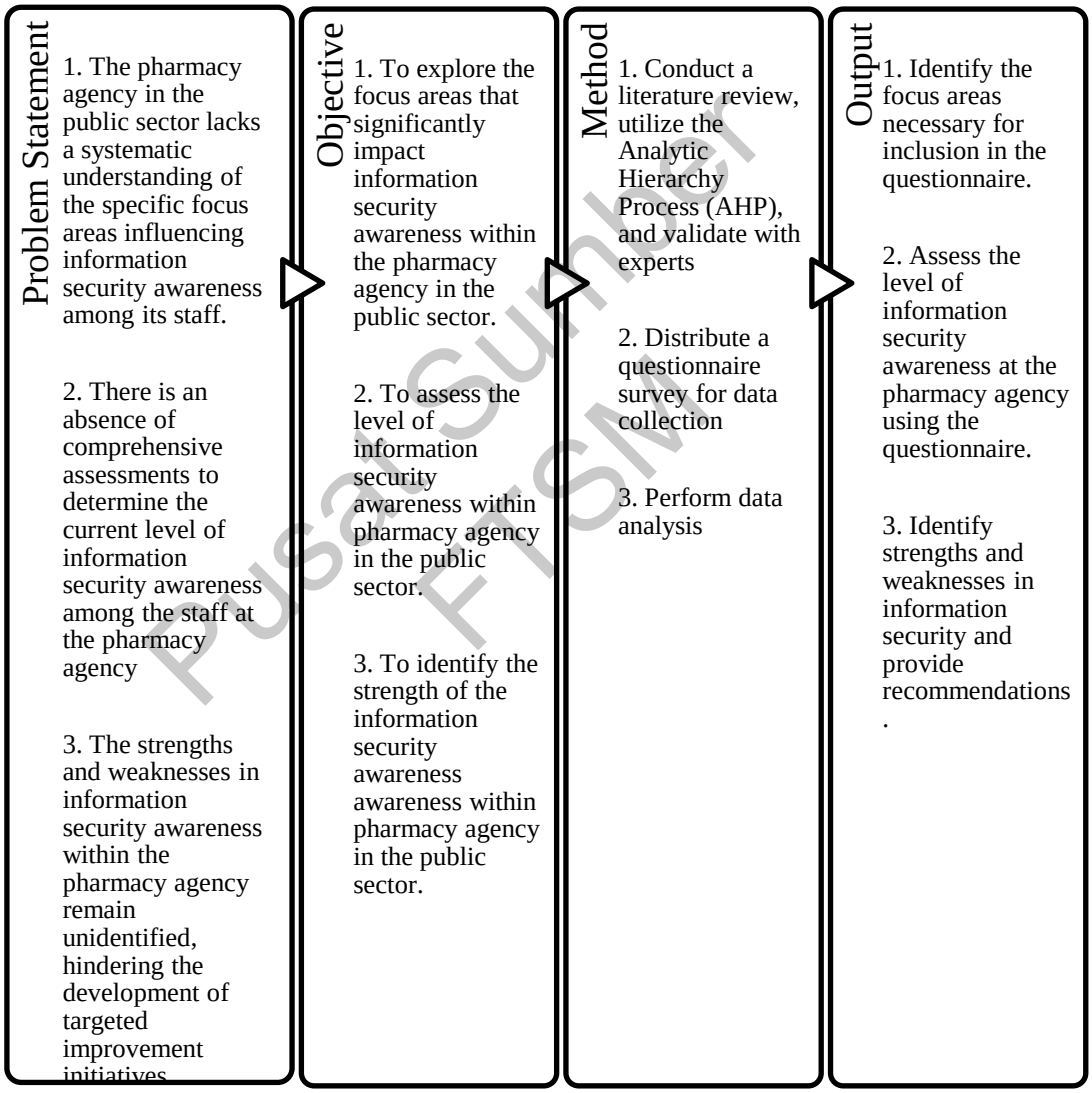

Figure 3.2 Mapping of the problem statement, objective, method and expected output.

Table 3.1 The nine focus areas

Focus Area	Items code	Sub-area
"Password management"	PM1	Using the same password
	PM2	Sharing passwords
	PM3	Using a strong password
	PM4	Securing a password
"Email use"	E1	Clicking on links in emails from known senders
	E2	Clicking on links in emails from unknown senders
	E3	Opening attachments in emails from unknown senders
"Internet use"	I1	Downloading files
	I2	Accessing dubious websites
	I3	Entering information online
"Social Media use"	SM1	Social media privacy settings
	SM2	Considering consequences
	SM3	Posting about work
"Mobile devices (including personal laptop, mobile phone etc.)"	MD1	Physically securing mobile devices
	MD2	Sending sensitive information via WIFI
	MD3	Shoulder surfing
"Information handling"	IH1	Disposing sensitive print outs
	IH2	Inserting removable media
	IH3	Leaving sensitive material
"Incidence reporting"	IR1	Reporting suspicious behavior
	IR2	Ignoring poor security behavior by colleagues
	IR3	Reporting all incidents
"Policy"	P1	Importance of an information security related policy in organization
"Training"	T1	Importance of training

3.3 QUESTIONNAIRE VALIDATION AND ANALYTIC HIERARCHY PROCESS

3.3.1 Expert Content Validity Test

The original version of HAIS-Q is available in Appendix A. As mentioned earlier, HAIS-Q can be modularly applied. Parsons et al. (2014) reported that the average time taken to complete the questionnaire in the pilot studies and main studies was 18 and 37 minutes, respectively. To minimize the risk of individuals not participating due to factors such as discouragement, our objective was to modify HAIS-Q. According to

Doorewaard & Tjemkes (2019), it is advisable to target for a duration of 10 minutes in questionnaire designing (Takens 2020). However, we aimed to strike a balance between achieving a reasonable completion time and collecting relevant data. To guide our decisions on which dimensions or focus area to include, we conducted an Analytic Hierarchy Process (AHP) and interviews with five subject matter experts (SMEs). SMEs, possessing extensive experience in the information security field, were expected to provide valuable input. During the AHP and validation, the primary focus was on a specific topic, i.e., the refinement of HAIS-Q. Our role was to facilitate the discussion, keeping it within the defined topic limits, and encouraging experts to openly share their perspectives.

Validating questionnaires and conducting Analytic Hierarchy Process (AHP) often entail the participation of numerous individuals with diverse and sometimes conflicting goals and interests. To facilitate effective decision-making in the realm of maintenance management, five experts were strategically divided into three distinct groups. The first group comprised the head of Information and Communication Technology (ICT) from the ABC, while the second group included two expert lecturers from the University Kebangsaan Malaysia, specializing in the education of Master of Cybersecurity. The third group consisted of two experts hailing from distinct private industries, each boasting over a decade of experience: one serving as the CEO of a cybersecurity firm, and the other as a cybersecurity team manager. This intentional division of expertise ensured a comprehensive and well-rounded perspective, incorporating insights from both academic and industry professionals, as well as the specific knowledge of the ICT head intimately familiar with the study context.

The validation process involves interviewing five individuals acknowledged as experts in the field of cybersecurity. These validation participants were presented with a questionnaire incorporating multiple focus areas derived from diverse standard literature studies and journals. Participants were tasked with evaluating the questionnaire's alignment with organization requirements and determining its appropriateness, providing reasons for their assessments. This feedback serves as valuable input for constructing a measurement model, subsequently incorporated into a

questionnaire for all employees. The outcomes of the adjustment to the measurement model are detailed in Appendix B.

Once the organization's measurement requirements are established, the subsequent phase involves defining the methodology for measurement. Kruger and Kearney employed the Analytic Hierarchy Process (AHP) to rank the dimensions and focus areas, providing a structured approach to prioritize and assess their significance (Kruger & Kearney 2006). This systematic process aids in determining the hierarchy of elements, contributing to a well-organized and informed decision-making process.

Based on expert evaluation, this research has developed a questionnaire comprising nine focus areas encompassing a total of 72 question item, which utilizing the HAIS-Q instruments and DKICT KKM. This expansion is driven by the literature review, underscoring the critical role of comprehending information security policies, participating in relevant training, and aligning with the guidelines set forth in DKICT KKM.

One more aspect to note is that in this questionnaire, we have introduced two additional focus areas: training and policy. However, it is evident that while previous focus areas within the HAIS-Q framework typically consist of three sub-focus areas each, the newly added “training” and “policy” focus areas contain only one sub-focus area each. This imbalance in the structure of the questionnaire raises concerns about potential data bias. Hence, we embarked on a literature review to explore this issue further.

Examples from previous studies, such as those conducted by Normandia et al. (2019) and Rosihan & Hidayanto (2022), demonstrate similar methodologies. Notably, the additional focus area of policy in these studies included only two sub-focus areas. Additionally, Nield et al. (2020) explored the GDPR focus area, which also had just one sub-focus area. Additionally, in a study by Gangire et al. (2021), which introduced the "privacy" focus area alongside the original HAIS-Q framework, but similarly encountered inconsistencies in the number of questions under each focus area. Despite

these discrepancies, their reliability analysis and correlation of factors yielded positive results.

The design of a questionnaire, from its visual layout to the wording of its questions, can significantly impact the data collected (Kasprzyk n.d.). Following the initial drafting of questionnaire items, it's recommended to enlist qualified experts to scrutinize the items for accuracy, absence of item construction issues, and grammatical correctness(Aithal & Aithal 2020). We send our questionnaire to a panel of experts to assess whether the questionnaire items effectively capture the intended construct and if they adequately cover the domain of interest.

The final stage in questionnaire development involves conducting reliability and validity tests (Tsang et al. 2017). Reliability, which pertains to the consistency of survey results, is assessed through measures like internal consistency, which gauges how closely questionnaire items correlate in measuring the same underlying construct(Aithal & Aithal 2020). Meanwhile, validity is established by ensuring the questionnaire accurately measures what it intends to. These tests, including Cronbach's alpha and the Pearson product-moment correlation coefficient, will help to gauge the internal consistency and assess the strength of relationships between variables, thereby ensuring the questionnaire's trustworthiness and effectiveness (Details in 3.6 Data Analysis).

3.3.2 Analytic Hierarchy Process

The Analytic Hierarchy Process (AHP) is a decision-making model that involves human subjects considered experts in their respective fields. AHP serves as a valuable framework for making informed decisions on complex issues (Normandia et al. 2019). In the AHP model, the human subject serves as the sole input. Expert criteria are individuals who possess a comprehensive understanding of the presented problem (Jajac & Bošnjak 2023). In determining the most pertinent priorities within the organization, the AHP was employed to rank each focus area effectively.

This approach is employed to identify and choose the most suitable alternatives, assessing them against multiple criteria. AHP finds application globally in diverse

problem scenarios within both private and government sectors (Rosihan & Hidayanto 2022). AHP represents a fundamental decision-making approach that integrates both rationality and intuition. It aims to facilitate the selection of the optimal choice among various alternatives connected through multiple criteria (Hermawan et al. 2022). In this process, each decision maker engages in pairwise comparison judgments, contributing to the determination of priorities or ratings for the alternatives. (Mahardika et al. 2020; Normandia et al. 2019).

Within the Analytic Hierarchy Process (AHP), the decision-maker performs straightforward pairwise comparisons, subsequently utilizing these assessments to establish comprehensive priorities that inform the ranking of alternatives (Prakoso et al. 2020). The most basic form of decision-making in this context involves a three-level hierarchy, where the top level represents the goal, the second level comprises the criteria, and the lowest level encompasses the alternatives as shown in figure 3.3.

To assign weights to the variables of the information security awareness focus areas, a pairwise comparison matrix was generated, allowing for a comprehensive assessment of the relative importance of the nine focus areas. The scale used ranged from 1, signifying equal importance between two variables, to 9, indicating absolute superiority of one variable over others. Once the pairwise comparison matrix was completed, the subsequent step involved calculating the eigenvalues, which represent the weights assig (Jajac & Bošnjak 2023; Normandia et al. 2019)jak 2023; Normandia et al. 2019).

The calculation of focus area weights involves the summation of values within each column in the matrix. Subsequently, each value in the column is divided by the total column sum to normalize the matrix (Hermawan et al. 2022; Normandia et al. 2019). Furthermore, the values within each row are summed and divided by the total elements to compute the average (Hermawan et al. 2022; Normandia et al. 2019). The outcomes of the focus area weights are elaborated upon in the following section.

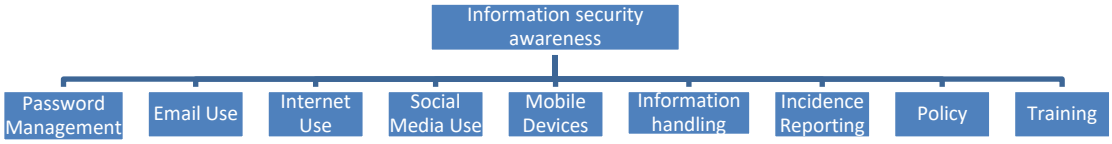

Figure 3.3 Analytical hierarchy process

3.4 PILOT TESTING

The pilot test involved 30 staff members at the ABC, utilizing the validated questionnaire provided by subject matter experts. The pilot test of the questionnaire revealed instances where certain questions lacked clarity, prompting the recommendation to include job level in the biographical section and remove the organization's section. The Cronbach alpha is carried out in pilot study and the value is more than 0.7 as shown in table 3.2.

Table 3.2 Cronbach alpha obtained in pilot study.

Dimension	Cronbach Alpha
Knowledge	0.867
Attitude	0.919
Behavior	0.860

3.5 DATA COLLECTION

The population comprises all personnel employed at ABC during the questionnaire distribution period, estimated to be around 500 individuals. With a margin of error 5%, confidence level of 95% and response rate 50%, the suggested sample size for the study is 218 respondents (Raosoft 2004). A total of 252 valid questionnaire responses are received. The majority of respondents are from non-IT backgrounds, with only a limited number of participants from the IT department. The research method involves administering a survey through email, using a Google Forms link. The survey begins with an introduction on the first page of the Google Form, which outlines the study's purpose and information. Participants are also presented with an informed consent form, which they must acknowledge by checking the "agree to continue" box. Subsequently, they are asked to provide basic demographic information, including gender, age, and job level, followed by the main survey questions.

Our research tools consist of questionnaires with a total of 72 questions, designed based on HAIS-Q. These questions aim to assess respondents' knowledge, attitudes, and behavior regarding information security awareness. The questionnaire focuses on seven specific areas of information security awareness and uses a 5-point Likert scale, ranging from 1 (strongly disagree) to 5 (strongly agree).

Of the 76 questions, 36 are negatively framed, and 36 are positively framed. For negative questions, "Strongly Disagree" scores 5 points, and "Strongly Agree" scores 1 point. Conversely, for positive questions, "Strongly Agree" earns 5 points, while "Strongly Disagree" scores 1 point.

Following the approach outlined by Parsons et al. (2017), inquiries related to KAB were distinctly provided, each accompanied by a brief introduction delineating its category. To prevent the inclusion of respondents who consistently respond in a uniform manner, questions were formulated both positively and negatively. A consistent response pattern across the entire questionnaire suggests a lack of attentiveness, warranting the exclusion of such participants from the final analysis. The accessibility of the questionnaire is extended over a three-week period post the distribution of invitations, with reminders sent each week.

3.6 DATA ANALYSIS

In the data analysis phase, various tests are conducted, including the Pearson Product Moment, Cronbach's alpha, descriptive statistical analysis, and Kruskal-Wallis. The details of each test are explained below.

Validation testing is conducted to assess the appropriateness of a question item in measuring the intended construct. The Pearson Product Moment technique is employed for validity testing. The Pearson correlation coefficients for all variables surpass the critical threshold of 0.124, as per the Pearson Critical Value Table (Oja 2021). This comparison is established considering a sample size of 250 and a significance level of 0.05 for a 2-tailed test. Reliability testing seeks to ascertain the degree of consistency in the measuring instruments, determining their reliability and stability when applied repeatedly. The Alpha-Cronbach technique is utilized for

reliability assessment. After establishing internal reliability, the subsequent step involves utilizing descriptive analysis to interpret the result. According to Chan and Idris (2017), a Cronbach's Alpha value above 0.7 is considered reliable (Chan & Idris 2017).

The collected data, providing information on the measurement level, and relationships among each dimension of information security awareness, undergoes processing through statistical tools such as SPSS 23 and Microsoft Excel. The AHP method determines the weight of focus area variables, while SPSS 23 facilitates descriptive statistical analysis and regression (Normandia et al., 2019). The interpretation can be used to pinpoint specific sub-areas of HAIS-Q that necessitate improvement in the ABC.

This study utilizes descriptive statistical analysis to gauge the level of awareness of employee's information security, represented in percentages. Subsequently, the average percentage for each dimension is computed by combining both the dimensional weights and the focus area weights. The weights assigned to the dimensional variables adhere to the criteria established by Kruger and Kearney (2006). Table 3.3 below presents an overview of the dimensional variable weights used in this research.

Table 3.3 Dimensional percentage

Dimension	Weight (%)
Knowledge	30
Attitude	20
Behavior	50

The assessment of information security awareness levels follows the methodology developed by Kruger and Kearney (2016) as shown in Table 3.4. Individuals are categorized into one of three levels based on their percentage scores:

1. A "Good Level" with a percentage score falling between 80-100%.
2. An "Average Level" with a percentage score in the range of 60-79%.
3. A "Poor Level" with a percentage score from 0-59%.

Table 3.4 Scale for information security awareness

Score (%)	Criteria	Information	Color Code
80-100	Good	"Satisfactory, does not require action/improvement"	
60-79	Average	"Monitor, potentially requiring action/improvement"	
0-59	Poor	"Unsatisfactory, requires action/improvement"	

The Kruskal-Wallis's test is employed in this study as a significant difference test, focusing on the evaluation of categorical variables. This statistical tool is commonly utilized to determine the significance of differences among two or more groups within a specified domain. The Kruskal-Wallis's test calculates a significant difference value and is particularly useful in scenarios where parametric assumptions are not met. As a non-parametric procedure, it relies on the ranking of observations rather than specific numerical values (Fadlika et al. 2023). In this study, the Kruskal-Wallis's test is applied to analyze the significant differences among different groups concerning the frequency of training, years of service and the total score of awareness across the three dimensions.

3.7 CONCLUSION

In conclusion, the methodology encompasses a comprehensive approach, starting with a literature review, followed by identifying the focus area, validation by experts, the use of the analytical hierarchy process to determine the weightage of each focus area, data collection, and data analysis. With this well-rounded methodology, the research on information security awareness in ABC is conducted with thoroughness and rigor.

CHAPTER IV

RESULTS AND DISCUSSION

4.1 INTRODUCTION

Chapter IV unfolds as a critical segment where the obtained results and subsequent discussions are intricately presented. This chapter serves as the analytical core of the study, revealing insights garnered from the application of the Analytic Hierarchy Process (AHP) in Section 4.1. Subsequently, the demographic characteristics of the respondents are examined in Section 4.2, providing a comprehensive overview of the study's participant profile. The robustness of the research methodology is evaluated through the presentation of validity and reliability test results in Section 4.3. Section 4.4 delves into the information security awareness levels, shedding light on the outcomes derived from the implemented measures. The statistical analysis of specific variables, as determined by the Kruskal-Wallis Test, is outlined in Section 4.5. The ensuing discussions in Section 4.6 dissect and interpret the results, offering a nuanced understanding of their implications. The chapter culminates with Section 4.7, where a set of recommendations is presented, aiming to guide future research endeavors and practical applications.

4.2 ANALYTIC HIERARCHY PROCESS (AHP)

Using the Analytic Hierarchy Process (AHP), eigenvalues were computed by assigning weights to each focus area, as depicted in Table 4.1.

The results reveal that Email Usage holds the highest significance with a value of 21.32%. This is attributed to the inherent nature of the correctional environment, where daily communication heavily relies on email. Employees are expected to

maintain a heightened awareness in email usage, exercising caution to avoid malicious links or downloading harmful attachments.

Password management follows as the second most crucial aspect with a weightage of 16.98%. Password management encompasses various sub-categories, including sharing passwords, using robust passwords, periodic password changes, and securing passwords. Internet usage ranks third, with a weightage of 14.3%. This focus area involves assessing and managing inappropriate internet use, as well as accessing non-work-related sites. Addressing these aspects is vital in mitigating potential information security threats related to internet activities.

Incidence reporting holds the fourth position, emphasizing the importance of promptly reporting any suspicious behavior or security incidents. A culture of reporting incidents contributes to the overall information security resilience of the organization. Information handling, social media use, policy adherence, mobile device security, and training are ranked from fifth to ninth, respectively.

The ninth focus area, Training, though assigned a lower weightage, remains pivotal in reinforcing information security awareness within the organization. Continuous training is deemed crucial, as it serves the vital purpose of keeping employees well-informed and prepared to confront the ever-evolving landscape of information security challenges. Despite its lower rank, the significance of Training is underscored by insights from subject matter experts.

According to one of the subject matter experts, there exists a proper channel for employees to request specific training sessions aligned with their interests and needs. This signifies a proactive approach within the ABC to cater to the diverse training requirements of the workforce. Additionally, the ABC demonstrates a commitment to information security preparedness by consistently organizing comprehensive training sessions on an annual basis.

Table 4.1 The percentage allocation for each focus area

Rank	Focus Area	Weightage (%)
1	Email	21.32
2	Password	16.98
3	Internet Use	14.3
4	Incidence reporting	11.02
5	Information handling	10.78
6	Social media use	7.32
7	Policy	7.02
8	Mobile devices	5.92
9	Training	5.34

4.3 DEMOGRAPHIC RESULTS OF RESPONDENTS

All respondents in this study were employees of the ABC. The questionnaire comprised 9 questions related to the respondents' background and 72 questions related to the dimensions of the KAB model and focus areas of the HAIS-Q, as previously defined. A detailed overview of the respondents is presented in Table 4.2 below:

Table 4.2 Demographics data

Variable	Items	Total	Percentage %
Gender	Female	188	74.6
	Male	64	25.4
Age	21-30	18	7.1
	31-40	187	74.2
	41-50	43	17.1
	51-60	4	1.6
Position	Pharmacist	190	75.4
	Assistant Pharmacist	36	14.3
	Office Secretary	5	2
	Information technology assistant	2	0.8
	Assistant Administrative	11	4.4
	Other	8	3.2

to be continued…

…continuation

Years of services	Less than 1	14	5.6
	1-3	36	14.3
	4-6	39	15.5
	7-10	78	31
	More than 10	85	33.7
How many information security related course have you attend during your services in ABC?	None	190	75.4
	1-3	58	23
	4-6	4	1.6
	7-10	0	
	More than 10	0	0
How many information security related course have you attend during the last three years?	None	199	79
	1-3	51	20.2
	4-6	2	0.8
	7-10	0	0
	More than 10	0	0
If you have ever attended information security course, please indicate the organizer of the course	None	177	70.2
	Government Organization	35	13.9
	ABC	19	7.5
	NGO/Private	9	3.6
	Other	12	4.8

The analysis of gender distribution in the survey reveals a noteworthy pattern common in the pharmacy sector, with a higher representation of female participants compared to male respondents. Specifically, females constitute a significant majority at 74.6%, while males make up 25.4% of the surveyed population. This gender composition aligns with prevailing trends observed in the pharmacy field, highlighting the predominance of female professionals in this sector.

In terms of age, most participants fall within the age range of 31-40, making up 74.2% of the respondents. Other age groups include 21-30 (7.1%), 41-50 (17.1%), and 51-60 (1.6%). The occupational breakdown reveals that the largest percentage, 75.4%,

holds the position of pharmacist, followed by assistant pharmacist (14.3%), office secretary (2%), information technology assistant (0.8%), assistant administrative (4.4%), and others (3.2%). Regarding years of service, the respondents exhibit a diverse range of experience. Notably, a considerable percentage has served for more than 10 years, constituting 33.7%, while those with 7-10 years of service make up 31%.

When it comes to information security training, a significant proportion of respondents (75.4%) have not undergone any training in the past services in the ABC, and a considerable majority (79%) have not received training within the last three years. Notably, despite a notable percentage (33.7%) of staff having more than 10 years of experience, none reported receiving training more than 10 times. The majority of respondents never attend training related to information security (70.2%), majority of respondents who attended information security courses received training organized by government organizations (13.9%), followed by ABC (7.5%), NGOs/private entities (3.6%), and others (4.8%). These insights provide a comprehensive overview of the demographics and c information security training landscape within the pharmacy regulatory body.

4.4 RESULT OF VALIDITY AND RELIABILITY TEST

The next step in the research process involved testing the questionnaires for both validity and reliability, aligning with the concepts elucidated in Chapter II. In the validity test, the correlation value of 0.124 (Oja 2021) was obtained, considering the 252 respondents. The questions were grouped to align with the KAB model factors used—Knowledge, Attitude, and Behavior. For detailed validation test results using the Pearson Product Moment, refer to the Appendix D.

Following the validity test, the research proceeded to reliability testing using the final dataset. Cronbach's alpha was employed as the test method, and similar to the validity testing, this test was conducted based on the three dimensions of the method used—Knowledge, Attitude, and Behavior.

Upon comparing the obtained correlation coefficient of 0.124 against the critical values in the table, while considering the degrees of freedom (d.f.), it was determined

that the observed correlation coefficient (r count) surpassed the critical threshold (r table) (Oja 2021). This comparison reaffirms the validity of each indicator in the validity test. The results indicate that the observed correlations are statistically significant and meet the criteria for establishing the validity of the questionnaire indicators.

Furthermore, the reliability test outcomes for each variable underscored their reliability, as evidenced by the calculated Alpha-Cronbach coefficients surpassing the accepted benchmark of 0.7, as depicted in Table 4.3. The Cronbach alpha values for each dimension are as follows: Knowledge (0.84), Attitude (0.92), and Behavior (0.91). These results contribute to the confidence in the robustness of the assessment tools, confirming that the indicators exhibit both validity and reliability, aligning with the study's objectives.

Table 4.3 Cronbach alpha value

Dimension	Cronbach alpha value
Knowledge	0.84
Attitude	0.92
Behavior	0.91

4.5 RESULT OF INFORMATION SECURITY AWARENESS LEVEL

Following the validation and reliability assessments, the next step involved measuring the level of information awareness for each focus area based on the utilized dimensions. The resulting percentage values are detailed in Table 4.4.

Table 4.4 Information security awareness measurement in percentage

Focus Area	Dimension				Total Awareness Level%
	Weightage, %	K (30%)	A (20%)	B (50%)	
Password management	16.98	84.27	82.86	82.00	82.85
Email use	21.32	78.41	80.79	82.06	80.71
Internet use	14.3	68.65	79.55	72.70	72.85
Social media use	7.32	77.14	81.90	79.95	79.50
Mobile devices	5.92	85.45	85.87	86.53	86.08
Information handling	10.78	85.03	84.66	86.88	85.88
Incidence reporting	11.02	76.22	79.89	78.23	77.96
Policy	7.02	77.86	78.57	67.94	73.04
Training	5.34	59.21	85.16	63.81	66.70
Total		77.74	81.74	78.95	79.15

The percentage values presented in the table 4.4 are derived from the averaging of each Knowledge (K), Attitude (A), and Behavior (B) variable within the specified focus areas. This comprehensive approach allows for a nuanced assessment of the awareness levels, considering the different dimensions that contribute to overall information security awareness.

Moreover, the total awareness section encompasses two perspectives: one based on the dimension distribution of weights by Kruger & Kearney, and the other based on the Analytic Hierarchy Process (AHP) weighting on focus are conducted. This dual perspective ensures a well-rounded evaluation, incorporating both expert judgment and a systematic analytical approach. The combination of these methodologies enriches the assessment, providing a more comprehensive understanding of the information security awareness landscape within the ABC.

The distinctions in the assessment columns highlight varying levels of information security awareness within each focus area, with the corresponding information available in table 3.4. The color-coded system serves as a visual representation, aiding in the interpretation of the c information security assessments.

The grey color signifies a good level of security awareness, indicating a satisfactory state of information security practices. Areas marked in grey suggest that the information security awareness in those aspects is commendable and meets the desired standards.

The green color, on the other hand, designates an average level of information security awareness. This suggests a monitoring status where certain actions may be considered to enhance awareness further. While not in a critical condition, these areas may benefit from proactive measures to address potential vulnerabilities.

Conversely, the red color indicates a poor level of information security awareness, signifying an unsatisfactory condition. In such cases, immediate and regular interventions are crucial to prevent the emergence of information security problems. The red-coded areas demand focused attention and targeted efforts to elevate awareness and fortify information security practices.

To elaborate on the information presented in the table 4.4, the overall information security awareness for the ABC is determined to be at a general score of 79.15%, categorizing it as a "monitor" level. This classification suggests that while the information security awareness is commendable, there is room for continuous observation and improvement.

Breaking down the awareness into specific dimensions, the knowledge dimension attains a score of 77.74%, the attitudes dimension scores 81.74%, and the behavior dimension receives a score of 78.95%. These individual dimension scores provide insights into the nuanced aspects of information security awareness, reflecting the strengths and areas for improvement within each dimension.

The holistic analysis, encompassing the overall awareness score, individual dimension scores, and specific focus area scores, offers a comprehensive understanding of the information security awareness landscape. This multifaceted approach serves as a valuable tool for targeted interventions and enhancements, addressing specific dimensions and criteria within the information security framework.

In the detailed examination of each variable, the assessment reveals a noteworthy distribution across three categories: "good," "average," and "poor." There are 13 parameters classified as "good," signifying a robust information security awareness performance in those aspects. Another 13 parameters fall under the "average" category, with a few registering percentage values that closely approach the "good" level. Additionally, one parameter is categorized as "poor," indicating an area that requires immediate attention and intervention.

When considering focus areas, four distinct categories emerge, namely "Password Management," "Email Usage," "Mobile Devices," and "Information Handling." These areas exhibit commendable performance, falling within the "good" category due to their total awareness percentages surpassing the 80% threshold. Notably, "Password Management," "Mobile Devices," and "Information Handling" stand out by achieving satisfactory performance across all Knowledge, Attitudes, and Behavior (KAB) dimensions. This underscores the effectiveness of these focus areas in promoting a high level of information security awareness within the organization.

Conversely, the remaining focus areas, including "Internet Usage," "Social Media Usage," "Incident Reporting," "Training," and "Policy," are categorized as "average." This classification indicates areas where potential actions or improvements are needed to enhance awareness levels.

The "Training" focus area exhibits a notable disparity in awareness across its KAB dimensions. Specifically, in the Knowledge dimension, the score stands at 59.2%, categorizing it as "unsatisfactory." In contrast, the "Training" focus area performs well in the Attitude dimension, scoring 85.16%. This indicates a positive perception among respondents regarding the benefits and preparedness gained from additional workforce

information security training. The Behavior dimension of "Training" registers a percentage of 63.81%, reflecting the level of engagement or willingness of respondents to attend or request training on information security or related topics. Although not as high as the Attitude dimension, the Behavior score still suggests a reasonably positive inclination toward participating in information security training activities.

The focus area exhibiting the second lowest total awareness, encompassing the KAB dimensions, is "Internet Use," which garnered an overall score of 72.85. Within this focus area, the breakdown reveals a knowledge score of 68.65%, indicating a moderate level of awareness regarding information security practices associated with internet use. On a more positive note, the Attitude score stands at 79.55%, reflecting a favorable perception among respondents regarding the importance and benefits of secure internet practices. The behavior dimension, with a score of 72.70%, suggests a moderate level of engagement in actual practices related to internet use and information security.

To gain a deeper understanding and identify areas of weakness, a comprehensive descriptive analysis of all items within each focus area was conducted. The specifics of this analysis are outlined in Table 4.5.

Table 4.5 Descriptive analysis of the items in focus area

		Knowledge		**Attitude**		**Behavior**	
Focus Area	Items	Mean	S.D	Mean	S.D	Mean	S.D
Password Management	PM1	4.19	0.915	4.12	0.901	4.29	0.720
	PM2	4.30	0.890	4.04	0.887	3.95	0.960
	PM3	4.31	0.875	4.13	0.931	4.31	0.715
	PM4	4.06	0.873	4.28	0.677	3.84	1.048
Email Use	E1	3.53	1.141	3.38	1.051	3.87	0.950
	E2	4.21	1.060	4.35	0.827	4.24	0.832
	E3	4.02	1.097	4.38	0.746	4.20	0.839
Internet Use	I1	3.15	1.164	3.92	0.836	3.34	1.119
	I2	4.00	0.943	4.19	0.63	3.65	1.001
	I3	3.14	1.155	3.82	0.951	3.92	0.868
Social Media Use	SM1	4.12	0.745	4.12	0.766	3.41	1.084

	SM2	3.33	1.115	3.9	0.909	4.18	0.782
	SM3	4.12	0.883	4.27	0.811	4.40	0.699
Mobile Devices	MD1	4.31	0.813	4.33	0.807	4.46	0.743
	MD2	4.13	0.948	4.25	0.851	4.31	0.774
	MD3	4.37	0.706	4.3	0.677	4.21	0.723
Information Handling	IH1	4.14	0.899	4.23	0.834	4.42	0.629
	IH2	4.40	0.876	4.45	0.784	4.40	0.764
	IH3	4.21	0.895	4.02	1.029	4.21	0.818
Incidence Reporting	IR1	4.16	0.624	4.1	0.808	4.04	0.661
	IR2	3.82	0.923	4.09	0.758	3.60	0.920
	IR3	3.46	1.188	3.8	1.026	4.10	0.643
Policy	P1	3.89	0.804	3.93	0.876	3.40	0.941
Training	T1	2.96	0.944	4.26	0.726	3.19	0.992

4.5.1 Training

a. Item-T1

For item T1, in the knowledge dimension (Mean = 2.96, S.D = 0.944), respondents indicate a relatively lower level of awareness regarding the consistent provision of information security management and training opportunities by their organization. The specific question about organizational provision of information security training suggests a potential gap in knowledge, highlighting the need for improved communication or accessibility of training resources within the organization.

In the attitude dimension (Mean = 4.26, S.D = 0.726), participants express a positive perspective, believing that the organization would benefit and be well-prepared against cyber-attacks through additional workforce information security training. This optimistic attitude reflects a recognition of the value of ongoing training in enhancing overall information security resilience.

In the behavior dimension (Mean = 3.19, S.D = 0.992), there is a lower score, indicating a tendency for respondents not to actively attend or request information security training. This discrepancy between positive attitudes toward training benefits and lower actual engagement in training activities suggests potential barriers or factors

influencing the decision to participate. Addressing these barriers and promoting the tangible advantages of information security training may help bridge the gap between positive attitudes and actual behavioral change, fostering a more security-conscious workforce.

4.5.2 Internet Use

a. Item-I1

For item I1, in the knowledge dimension (Mean = 3.15, S.D = 1.164), respondents seem moderately uncertain about their organizational policy on downloading files for work purposes. The specific question about being allowed to download files onto the work computer if they help in doing the job suggests a need for clarity or communication regarding this policy. In contrast, the attitude dimension (Mean = 3.92, S.D = 0.836) reflects a high level of concern about the potential risks associated with downloading files at work. This indicates a cautious mindset among participants. In terms of behavior (Mean = 3.34, S.D = 1.119), respondents exhibit a moderate level of engagement in downloading files for work-related tasks, suggesting a balance between adherence to policy and the practicalities of job performance.

b. Item-I2

In the knowledge dimension (Mean = 4.00, S.D = 0.943), participants exhibit a strong understanding of the organizational policy, particularly related to internet use. Specifically, participants acknowledge the restriction on accessing certain websites while on duty, reflecting a conscientious awareness of company guidelines. However, in the behavior dimension (Mean = 3.65, S.D = 1.001), there is a noteworthy dip in scores, indicating a more conservative approach needed to visiting websites during work hours. The specific question of I2 about freely accessing any websites at work points to a cautious behavior among respondents, aligning with the positive yet guarded attitude (Mean = 4.19, S.D = 0.63) observed in the data. The overall picture suggests a careful balance between KAB dimensions concerning internet use, with participants being aware of potential risks.

c. Item-I3

For item I3 in the knowledge dimension (Mean = 3.14, S.D = 1.155), respondents display a moderate level of uncertainty or lack of clarity about entering information on any website for job-related purposes. The specific question about being allowed to enter information on any website if it helps in doing the job highlights a potential need for clarification or communication on this aspect of organizational policy. The attitude dimension of I3 (Mean = 3.82, S.D = 0.951) reflects a positive inclination toward entering information on websites if it aids job performance, regardless of content. In the behavior dimension (Mean = 3.92, S.D = 0.868), participants demonstrate a cautious approach, with a high level of safety assessment before entering information on websites. This suggests a conscious effort to balance the practical needs of the job with the importance of ensuring the safety of online activities.

4.5.3 Policy

a. Item-P1

In the knowledge dimension (Mean = 3.89, S.D = 0.804), respondents display a moderate awareness of the organization's ICT security policy, specifically DKICT in the Ministry of Health. This indicates a baseline understanding of the existing policy within the organization. In the attitude dimension (Mean = 3.93, S.D = 0.876), the relatively lower score suggesting that they believe the ICT security policy is primarily applicable to the ICT department and not directly relevant to their job scope. This perspective may influence how individuals perceive and interact with the policy, potentially impacting their adherence.

In the behavior dimension (Mean = 3.40, S.D = 0.941), there is a lower score, indicating a decreased frequency in periodically reviewing and refreshing understanding of the DKICT KKM policy or related policies. The specific question about reviewing the policy aligns with organizational information security goals, suggesting a potential gap in actively staying informed about information security measures. This discrepancy between KAB dimensions underscores the need for targeted

efforts to enhance awareness and emphasize the relevance of the ICT security policy across all job scopes within the organization.

4.5.4 Incident Reporting

a. Item-IR1

In the knowledge dimension (Mean = 4.16, S.D = 0.624), respondents exhibit a strong understanding of incident reporting, particularly related to recognizing and reporting security incidents. The attitude dimension (Mean = 4.1, S.D = 0.808) reflects a positive attitude toward the importance of reporting incidents. However, in the behavior dimension (Mean = 4.04, S.D = 0.661), there is a slightly lower score, indicating a moderate level of engagement in actually reporting incidents. While knowledge and attitude are high, there may be room for improvement in translating that understanding into consistent reporting behaviors.

b. Item-IR2

In the knowledge dimension (Mean = 3.82, S.D = 0.923), participants express awareness of the need to address poor security behavior by colleagues. However, the behavior dimension score (Mean = 3.60, S.D = 0.920) is relatively lower, suggesting a hesitancy or reluctance to take action when noticing colleagues ignoring security rules. This discrepancy between knowledge and behavior highlights a potential gap in the application of knowledge to real-world scenarios. It may be valuable to explore factors influencing this observed hesitation in addressing security behaviors within the workplace.

c. Item-IR3

In the knowledge dimension (Mean = 3.46, S.D = 1.188), respondents indicate a moderate understanding of the optional nature of reporting security incidents. In the attitude dimension (Mean = 3.8, S.D = 1.026), participants recognize the risks associated with ignoring security incidents, even if they perceive them as not significant. The behavior dimension (Mean = 4.10, S.D = 0.643) shows a relatively higher score, suggesting a proactive approach to reporting security incidents when

noticed. This positive behavior aligns with the recognition of the risks associated with ignoring security incidents, indicating a strong commitment to maintaining a secure work environment.

4.5.5 Social Media Use

a. Item-SM1

In the knowledge dimension (Mean = 4.12, S.D = 0.745), respondents show a strong understanding of social media privacy settings. However, in the behavior dimension (Mean = 3.41, S.D = 1.084), there is a notable dip in scores, indicating a lower frequency of regularly reviewing social media privacy settings. The specific question about not regularly reviewing privacy settings points to a potential gap in actual practices compared to knowledge levels. It suggests that while participants are aware of privacy settings, they might not be consistently implementing privacy checks.

b. Item-SM2

In the knowledge dimension (Mean = 3.33, S.D = 1.115), respondents display a moderate level of awareness regarding the consequences of social media posts. The specific question about not being fired for social media posts suggests some uncertainty or lack of clarity on organizational policies. In the attitude dimension (Mean = 3.9, S.D = 0.909), participants express a relatively neutral stance, indicating a balanced perspective on posting content on social media that they wouldn't normally say in public. In terms of behavior (Mean = 4.18, S.D = 0.782), respondents exhibit a higher score, suggesting a tendency to post content on social media that they might not express publicly, indicating a certain level of comfort or freedom in online expression.

c. Item-SM3

In the knowledge dimension (Mean = 4.12, S.D = 0.883), respondents demonstrate a strong awareness of the freedom to post work-related content on social media. The attitude dimension (Mean = 4.27, S.D = 0.811) reflects a balanced perspective, acknowledging the risks associated with posting certain work-related information. Interestingly, the behavior dimension (Mean = 4.40, S.D = 0.699) shows a high level of

confidence or willingness to post whatever one wants about work on social media. This suggests a potential gap between knowledge and behavior, with users expressing a cautious attitude but demonstrating a more liberal approach in their actual online actions.

4.6 KRUSKAL WALLIS TEST

The application of the Kruskal-Wallis test aims to investigate the presence of statistically significant differences not only between training frequency and awareness score but also between years of service and awareness score. This non-parametric test is chosen for its ability to explore potential variations among multiple groups, shedding light on whether the observed differences in the specified variables are likely attributable to systematic factors rather than mere random chance.

4.6.1 Kruskal-Wallis Test for Training Frequency and Awareness Score

Table 4.6 Descriptive analysis of KAB score and frequency of training.

	N	Mean	Std. Deviation	Minimum	Maximum
Knowledge total score	252	94.34	10.514	71	117
Attitude total score	252	98.66	12.047	69	120
Behavior total score	252	95.94	11.602	71	120
How many information security related course have you attend during your services in ABC?	252	1.26	.475	1	3

Table 4.7 Mean rank of KAB score according to frequency of training.

Dimension	How many information security related course have you attend during your services in ABC?	N	Mean Rank
Knowledge	0	190	122.25
	1-3	58	139.21
	4-6	4	144.13
Attitude	0	190	124.34
	1-3	58	132.77
	4-6	4	138.25
Behavior	0	190	123.21
	1-3	58	136.18
	4-6	4	142.38

Table 4.8 Kruskal Wallis Test for training frequency and awareness score

Test Statistics[a,b]

Dimension	Knowledge	Attitude	Behavior
Kruskal-Wallis H	2.646	.700	1.602
df	2	2	2
Asymp. Sig.	.266	.705	.449

a. Kruskal Wallis Test

b. Grouping Variable: How many information security related course has you attend during your services in ABC?

A comprehensive analysis was conducted using the Kruskal-Wallis test to investigate potential differences among participants in the ABC based on the number of information security courses attended. The distribution of participants across groups revealed a notable imbalance, with Group 0 (attended 0 courses) having a significantly larger number of participants (190) compared to Group 1-3 (attended 1-3 courses) with 58 participants and Group 4-6 (attended 4-6 courses) with only 4 participants. This skewed distribution, where the majority of participants fall into Group 0, may impact the overall results, given that statistical tests such as the Kruskal-Wallis consider the ranks of observations. The mean rank is assigned to each group according in table 4.6.

In the assessment of Knowledge, participants attained an average score of 94.34, showcasing notable variability, as evidenced by a standard deviation of approximately 10.514. For Attitude, participants, on average, achieved a score of approximately 98.66, indicating variability in attitude scores, as reflected by a standard deviation of about 12.047. Turning to Behavior, the average total score slightly decreased to 95.94, and the standard deviation of 11.602 indicated variability in observed information security related behaviors. The mean descriptive is shown is table 4.5.

These findings signify significant variability in knowledge levels, with individual differences contributing to the dispersion in scores, thereby highlighting diverse knowledge levels among participants. The results of the Kruskal-Wallis test in table 4.7 showed no significant differences in the ranks of Knowledge and Attitude total scores among groups based on the number of information security courses attended. Similarly, for behavior total score, the test did not reveal significant differences among groups.

In summary, participants in ABC exhibited diverse levels of engagement in information security, reflected in variations in knowledge, attitude, and behavior scores. Notably, the number of information security courses attended did not emerge as a significant explanatory factor for observed differences, as evidenced by the non-significant results of the Kruskal-Wallis test. The disproportionate representation of participants in this group and other statistical considerations may significantly influence the impact of certain groups on the overall results. Further analysis and exploration of these statistical nuances are recommended to ensure a robust understanding of the information security landscape within ABC.

4.6.2 Kruskal-Wallis Test for Service Tenure and Awareness Scores

Table 4.9 Descriptive analysis of KAB score and service tenure.

	N	Mean	Std. Deviation	Minimum	Maximum
Knowledge total score	252	94.34	10.514	71	117
Attitude total score	252	98.66	12.047	69	120
Behavior total score	252	95.94	11.602	71	120
Service tenure	252	3.73	1.223	1	5

Table 4.10 Mean rank of KAB score according to service tenure.

Dimension	Service tenure	N	Mean Rank
Knowledge	Less than 1	14	141.04
	1-3	36	124.36
	4-6	39	120.59
	7-10	78	121.61
	more than 10	85	132.21
Attitude	Less than 1	14	127.04
	1-3	36	127.50
	4-6	39	106.88
	7-10	78	122.39
	more than 10	85	138.76
Behavior	Less than 1	14	132.29
	1-3	36	135.69
	4-6	39	118.27
	7-10	78	119.58
	more than 10	85	131.78

Table 4.11 Kruskal Wallis Test for service tenure and awareness score

Test Statistics[a,b]

Dimension	Knowledge	Attitude	Behavior
Kruskal-Wallis H	1.719	5.489	2.308
df	4	4	4
Asymp. Sig.	.787	.241	.679

a. Kruskal Wallis Test

b. Grouping Variable: Service tenure

The descriptive statistics provide an overview of participants' Knowledge, Attitude, and Behavior total scores, along with their service tenure in the ABC. On average, participants demonstrated a knowledge total score of 94.34 (SD = 10.514), an Attitude total score of 98.66 (SD = 12.047), and a Behavior total score of 95.94 (SD = 11.602). The details in table 4.8.

Participants were categorized based on service tenure into groups labeled as "Less than 1 year," "1-3 years," "4-6 years," "7-10 years," and "more than 10 years." Mean ranks were assigned to each group for KAB dimensions total scores in table 4.9.

The Kruskal-Wallis tests in table 4.10 were conducted to examine whether there were significant differences in scores among different service tenures. For Knowledge total score, the test yielded a non-significant result ($H = 1.719$, $df = 4$, $p = 0.787$), indicating no significant variation in Knowledge scores across service tenures. Similarly, for Attitude total score, the test result was non-significant ($H = 5.489$, $df = 4$, $p = 0.241$), suggesting no significant differences in Attitude scores among service tenure groups. The Kruskal-Wallis test for behavior total score also produced a non-significant result ($H = 2.308$, $df = 4$, $p = 0.679$), indicating no significant variation in Behavior scores across different service tenures. In summary, the analyses suggest that there are no significant differences in Knowledge, Attitude, or Behavior scores based on service tenure in the ABC.

In this study, the scale of service tenure utilized, ranging from less than 1 year, 1 to 3 years and small increments, thereafter, was deliberately chosen to facilitate a detailed examination of the impact of service tenure on information security awareness. This approach offers the opportunity to explore how awareness evolves over shorter time frames, including the critical early years of employment compared to later stages. While this granularity enhances the study's depth, it also presents challenges. The smaller increments may lead to smaller sample sizes within each tenure group, potentially compromising the statistical power of the analysis.

In future iterations or expansions of this study, it will be crucial to carefully assess the demographics of the study site and determine the most appropriate scale of service tenure to accurately evaluate whether service tenure significantly influences information security awareness scores. While the current study's approach of utilizing smaller increments in service tenure offers a detailed examination of the impact on information security awareness, it's important to recognize the potential limitations, particularly regarding sample sizes and the ability to discern significant differences between tenure groups. By conducting a thorough assessment of the study site demographics, researchers can tailor the scale of service tenure to better suit the population under investigation. This consideration will ensure that the study remains robust and provides meaningful insights into the relationship between service tenure and information security awareness.

4.7 DISCUSSION

Based on the analysis of respondents' answers to the questionnaire, several factors influencing awareness enhancement are evident. The following discussion focuses on the five weakest areas, ranging from the lowest to the highest scores: “training”, “internet use”, “policy”, “incidence reporting”, and “social media use”. The collective analysis across all dimensions provides insights into the varying levels of awareness and perceptions surrounding information security, highlighting potential areas for improvement and strategic focus.

4.7.1 Training

In the Knowledge Dimension, the awareness score for "training" stands at 59.2%, indicating a lower level of awareness. The questions in this dimension likely focused on key aspects, such as consistent information security management and the organization's provision of training in workforce information security. Moving to the Attitude Dimension, the awareness score for "training" is notably higher, reaching 85.16%. This dimension evaluates whether respondents perceive benefits and feel prepared for potential cyber-attacks with additional workforce information security training. In the Behavior Dimension, "training" achieved a score of 63.81%. This dimension explores whether respondents actively attend or express a desire to attend training sessions on information security or related topics. The findings emphasize the importance of consistently providing information security training and managing information security effectively to improve overall awareness.

Communication gaps pose a significant challenge in the awareness of information security training within the organization (Neigel et al. 2020). Ineffectively communicating the importance of consistent information security management and the availability of training programs may contribute to a lack of awareness among respondents. This deficiency in communication hinders employees from fully grasping the critical role that information security practices play in maintaining a secure organizational environment(Rosihan & Hidayanto 2022). Without a clear understanding of the significance of these practices, awareness remains limited, impacting the overall score in the Knowledge Dimension.

Additionally, limited accessibility to training resources exacerbates the awareness issue. If the organization fails to provide easily accessible and well-promoted training resources, employees may remain unaware of available opportunities. This lack of awareness can result in lower participation rates, as employees are not adequately informed about the avenues for skill development and information security training within the organization.

Furthermore, the inadequacy of training programs contributes to the awareness challenge(Rajamaki et al. 2018). If the content and effectiveness of the training programs fall short or are not tailored to address the specific needs of the workforce, awareness diminishes(Pattinson et al. 2018; Rajamaki et al. 2018). Employees may perceive the training as irrelevant or insufficient in addressing their information security knowledge gaps, thereby impacting the overall awareness score.

Lastly, the absence of mandatory training requirements exacerbates the issue(Pattinson et al. 2020; Rajamaki et al. 2018). When information security training is not made mandatory or emphasized as a crucial component of job responsibilities, employees may deprioritize participation. This lack of emphasis on mandatory training contributes to lower awareness levels, as employees may not recognize the necessity of staying informed and educated on information security practices.

4.7.2 Internet Use

In the context of "Internet Use," all three dimensions have been classified as "Monitor," resulting in a total awareness score of 72.854497%. The analysis suggests that awareness scores in the knowledge dimension may be influenced by factors related to understanding the risks associated with internet use and adopting safe online practices. While the overall scores in KAB dimensions indicate a positive attitudes toward internet use, there is room for improvement. Efforts can be directed towards enhancing knowledge levels to ensure users are well-informed about the potential risks and benefits of internet use. This holistic approach aims to bridge the identified gaps and foster a more secure and informed internet usage culture within the organization.

The factors that impact awareness and utilization of the internet, particularly within the "Internet Use" focus area, are multifaceted. A notable factor contributing to lower awareness is the prevailing lack of proportional increase in user literacy, despite the widespread availability of accessible and free internet usage (Hermawan et al. 2022). Users may not be adequately equipped to navigate the internet safely and responsibly, ultimately impacting their overall awareness.

Additionally, there exists a lack of clarity regarding the global extent to which individuals can effectively operate the internet according to their needs (Hermawan et al. 2022). This unclear perception may lead users to engage in online activities without a comprehensive understanding of associated risks, further diminishing their awareness levels.

Furthermore, the perceived freedom in seeking assistance for necessary tasks on the internet is another factor influencing awareness. This sense of freedom can lead individuals to engage in activities without fully recognizing the inherent risks, contributing to behaviors that compromise information security and influencing the overall awareness score (Yeo et al. 2023).

4.7.3 Policy

The analysis of the "Policy" dimensions reveals awareness scores of 77.86% for Knowledge, 78.57% for Attitude, and 67.93% for Behavior. Notably, in the Behavior dimension, respondents were questioned about their periodic review and refreshment of policies to align with organizational information security goals.

Several factors contribute to the observed low awareness of organizational policies. Firstly, the complexity of policy content presents a challenge, making comprehension difficult for individuals(Lee & Ariffin 2021). Addressing this issue involves ensuring that policies are written in clear and accessible language. Secondly, a perceived lack of relevance to daily job responsibilities can diminish motivation for engagement. Therefore, it is crucial to emphasize the policy's direct relevance to individual roles.

Moreover, if the organizational culture does not prioritize policy awareness, employees may not consider it a priority. Cultivating a culture that values and emphasizes policy awareness is vital for organizational security(Parsons et al. 2015; Wiley et al. 2020). Lastly, limited recognition of the policy's importance within the organization can contribute to low awareness. Effectively communicating the critical role of the policy in achieving organizational security objectives is essential for fostering a culture of informed and compliant employees.

While knowledge and attitude scores are relatively high, the behavior score indicates a moderate level of adherence to policy review and refreshment. This suggests that there is a positive perception of the policy's relevance to daily job responsibilities, highlighting its importance in the organizational context. To enhance policy adherence, efforts can be directed toward simplifying policy language, emphasizing relevance, fostering a culture of awareness, and consistently communicating the policy's significance within the organization.

4.7.4 Incidence Reporting

In the realm of "Incidence Reporting," all dimensions showcase remarkably similar percentages: 76.22% for Knowledge, 79.89% for Attitude, and 78.23% for Behavior, culminating in a total awareness score of 77.96%.

A notable causal factor influencing awareness in this dimension is the prevalent high sense of trust among employees. This trust dynamic may contribute to a tendency among individuals not to report mistakes made by their coworkers (Hermawan et al. 2022). Recognizing the need for improvement in consistently reporting incidents, even within a high-trust environment, is identified as a critical area for future enhancement(Cindana & Ruldeviyani 2019). Addressing this factor holds the potential to cultivate a more comprehensive and proactive approach to incidence reporting within the organizational context. Efforts to foster a reporting culture that values transparency and accountability can contribute to heightened awareness and improved incident reporting practices.