STAP
Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Adaptation and Validation of the KAB Model to Assess the Risk of Internal Information Security Incidents

Amjad Mahfuth[1*], Salman Yussof [2*]

[1]*College of Computer Science and Information Technology, Al-Quds Open University, Tulkarm West Bank, Palestine*

[2] *Institute of Informatics and Computing in Energy, Universiti Tenaga Nasional, Putrajaya, Malaysia*

ARTICLE INFO

Article History

Received: 01-05-2026
Revised: 30-05-2026
Accepted: 27-06-2026
Published: 12-08-2026

Vol.2026, No.3

DOI:

Corresponding author.
Email:
amahfouth99@gmail.com and *Salman@uniten.edu.my*

Orcid:

https://orcid.org/0000-0003-2583-4696

ABSTRACT

Many studies have revealed that an organization's insiders pose risks to the security of information assets. Among the key threats to a secure information environment are employees' actions and behaviors in handling information. Insiders, whether intentional or unintentional, may pose significant risks, despite the substantial investments organizations typically make in security controls and related solutions. Employee behavior in information security cannot be fully addressed through technical and procedural controls alone. An organization's approach to information security should include employee behavior because the organization's success or failure effectively depends on what its employees do or fail to do. To develop appropriate security perceptions between employees within an organization, we need to know the security knowledge required to influence employee behavior. To achieve this, the KAB (knowledge, attitude and behavior) model has been adapted and validated to guide the cultivation of a security culture that helps minimize internal security threats in organizations. The literature review indicated a positive relationship between knowledge and behavior. Accordingly, this research aims to investigate the security knowledge required to influence employee behavior and to examine the impact of security knowledge on behavior. This research uses a questionnaire was used to collect the data from the employees. The result of the quantitative analysis revealed that the knowledge of security threat, knowledge of security risk, knowledge of security responsibility and knowledge of legislation, regulation and national culture have significant effect on employee behavior. Furthermore, the result has also shown that these knowledge security construct have significant positive indirect effect on behavior through attitudes. These areas of security knowledge should be incorporated as key topics in organizational security training and awareness programs for employees, in order to foster an effective information security culture within the organization.

Keywords: KAB Model, Insider threat, Security Behavior, Information Security Culture, Security Knowledge, Security behavior, Organization.

How to cite the article

1. INTRODUCTION

Information is a critical asset for organizations [1]. Protecting it is crucial to ensure the stability of the organization and to maintain the availability, integrity, and confidentiality of that information. A recent study by the Ponemon Institute (2022) indicates that many organizations have lost billions of dollars as a result of information breaches or violations. Among the major threats faced by organizations are employees' actions and behaviors, especially when they interact with the organization's assets. Research on data breach investigation reports indicates that employees within organizations are responsible for most data breaches, whether intentionally or unintentionally [2]–[5]. Moreover, many studies [6]–[10] have concluded that insiders can pose significant threats to the security of information within an organization.

In information security, human error and negligence contribute to most data breaches in organizations [11]–[14]. Focusing solely on technical measures to protect an organization's assets without considering the human factor is clearly inadequate [12],[15]. Employees play a prominent role in creating threats to an organization and in preventing them. Therefore, organizations should focus on employees' behavior, attitudes, knowledge and awareness to establish an information security culture. The effectiveness of any security system depends on employees' behavior toward the organization's information assets [10], [16]-[18]. Employee behavior refers to the way employees conduct their work, either positively or negatively [17]. It may significantly affect an organization's information security effectiveness.

2. Literature Review

Information Technology has become an invaluable asset in most aspects of life, business, industries, organizations, governments and other sectors. This transformation leads to most organizations adopting the technology to perform daily tasks. Consequently, these changes have introduced a lot of risks to user and organizational information assets. Therefore, the organizations need to enhance their information security capability to protect the organization's assets and respond to new challenges and risks to ensure the stability and continuity of the organization. In general, most organizations have made the efforts to manage information security by focusing on the technology and process. Most organizations spend their money on technical measures and security products [18], [19] . However, not many organizations spent money on the management of human behavior in terms of providing information security between the employees. An organization's approach to information security should focus on employee behavior, as the organization's success or failure effectively depends on the things that its employees do or fail to do.

Establishing an information security culture within an organization can reduce the harmful interaction of employees towards organization's information assets. Furthermore, it will reduce the risk of employee misbehavior when they interact with the organization's assets [2],[9],[20],[21]. Information security culture guides how things are done in organization in regard to information security, with the aim of protecting the information assets and influencing employees' security behavior [22]. According to the broader literature [23]-[25], information security culture is defined as the result of security behavior. Accordingly, this study adopts the definition that security behavior, when practiced consistently over time, establishes an information security culture. This definition is chosen because of the relationship between knowledge and behavior as documented by [26], [27]. Knowledge and behavior are recognized as significant factors in information security culture studies [22],[26],[28], where knowledge guides employees' behavior, and consistent practice of this behavior over time establishes an information security culture.

In this paper, the KAB model has been adopted that matches the relationship assumptions between knowledge and behavior is the model. The related studies concerning the use of KAB model in information security was gathered using systematic review and analyzed using qualitative content analysis. A thorough review of literature highlighted papers dedicated to KAB model in information security that discuss use of KAB model, the development of KAB model or the proposal of model to enhance the KAB model in information security. All the studies that used KAB model in order to examine the relationships between knowledge, attitude and behavior are in the field of information security awareness.

[28] proposed KAB model for assessing information security awareness in an international mining company. They measured the effectiveness of information security awareness program on the basis of knowledge, attitude and behavior. This aims to ensure that their employees are informed and aware of security risks, thereby protecting themselves and their profitability. The proposed tool was based on techniques borrowed from the field of social psychology that proposes that learned predispositions to respond in a favorable or unfavorable manner to a particular object have three components: affect, behavior

and cognition. These three components were used as a basis and the model was developed on three equivalent dimensions namely what does a person know (knowledge), how do they feel about the topic (attitude) and what do they do (behavior).

[28] focused on the following six risk categories: always adhere to company policies, keep passwords and personal identification numbers secret, use e-mail and the Internet with care, be careful when using mobile equipment, report incidents like viruses, thefts and losses and be aware, all actions carry consequences. As a first classification of what to measure, it was decided to measure the three dimensions which are: knowledge, attitude and behavior. Each one of these dimensions was then subdivided into the six focus areas and on which the awareness program was based. Such model of divisions and subdivisions aim to measure information security awareness based on the proposed KAB model.

[29] proposed a model which is the integration of knowledge-attitude-behavior (KAB) with factors of theory of planned behavior TPB to influence the employee behavior. The proposed model includes knowledge, attitude, norms, intention of behavior and actual change in behavior. The KAB model, by itself is not sufficient to bring change in attitude and behavior for long term. In order to understand the change in attitude and behavior and how a change in attitude leads to change in behaviour he borrowed some elements from Theory of Planned Behavior (TPB). This theory explains relation between attitude and behavior and includes both the direct attitude-behavior path as well as an indirect attitude-intention-behavior path. The proposed model takes the knowledge attribute from the KAB model, attitude and social norms from the theory of planned behavior to achieve the desired change in behavior. Finally, the author suggested the following methods for effectiveness of information security awareness namely, educational presentation, e-mail messaging, group discussions, newsletter articles, video games, computer-based training and poster. The author concluded that providing information security awareness campaigns based on the proposed model have the ability to change user's behaviour and hence raise user's information security awareness.

[30] reports awareness of information security at a small and medium enterprise in Malaysia based on KAB model. To establish the relationship between knowledge, attitude and behavior in information security awareness among the employees in terms of availability, confidentially and integrity, a survey questionnaire was used to collect data. The findings revealed that attitude and behavior have significant influence on confidentiality, integrity, and availability of business information while knowledge was found to be not significant to availability.

[31] developed a tool based on KAB model to produce an empirically validated instrument, known as the Human Aspects of Information Security Questionnaire (HAIS-Q). This tool includes specific items to measure each factor in KAB model, for example, organizational factors are measured via organizational and security culture, subjective norms, rewards and punishments in order to develop KAB model. This tool could be used to measure employee knowledge, attitude and behavior to provide management with a benchmark. The aim of the paper is to outline the development of HAIS-Q and to examine the relationships between knowledge of policy and procedures, attitude towards policy and procedures and behavior when using a work computer. They used the model in seven focus areas: internet use, email use, social networking site use, password management, incident reporting, information handling and mobile computing.

[32] proposed an evaluation method for human aspects of information security that uses an online framework in order to give employees fast and personalized feedback on their self-report based on KAB model across different focus areas. An empirical study is performed to aid in validating the proposed evaluation method for human aspects of information security. In this study, knowledge, attitude and behavior in KAB model are measured in seven focus areas. These areas are: password management, e-mail use, internet use, social networking site use, incident reporting, working remotely, information handling.

[33] provided methods of training awareness in the field of information security that aims to mitigate the risks of information security. The aim of the study was to present the essence and importance of information security awareness as well as to analyses selected methods used in forming the employee awareness in information security. The author suggested methods for forming security awareness for employees namely, traditional methods, educational game and films, and internet method. The author concluded that information security awareness is a dynamic process, dependent on ever-changing threats. It is therefore considered that any safety awareness program should be subjected to continuous monitoring, thus forming an integral part of the company's culture. Finally, the author suggested the use of KAB model to explain the role of knowledge in behavior change. The analysis of study shows that the increasing employee awareness of information security is largely dependent on the method of providing knowledge. In addition, the literature studies have confirmed that awareness-raising methods and techniques, such as trainings and communication, are effective in enhancing user safety knowledge, including promotion of appropriate attitudes and behavior.

[34] evaluated the information security awareness for informatics student based on KAB model in order to guide university to formulate information security awareness program for their students based on the result of this study. In this study modifies six focus areas that adopted from Human Aspects of Information Security Questionnaire (HAIS-Q), in which each sub-focus area is expanded into three criteria using Knowledge- Attitude-Behavior based on KAB model. The author found that there is a positive relationship between knowledge, attitude and behavior with respect to ISA measurement.
[35] proposed a model called as enhanced Knowledge-Attitude-Behavior (KAB). The knowledge in KAB model was enhanced to include an e-learning element. This is to investigate the function of e-learning in enhancing the awareness level for simple and faster understanding. E-learning element also includes presentations with video clips on spear phishing, available online through open learning and phish awareness blog for enhance self-study by user. The name of the developed model is ISA KAB model (Information Security Awareness, knowledge, attitude and behavior) model. The aim of the model is to raise the awareness level among students and to investigate the awareness level of phishing attacks on the targeted group of vocational students.
[36] examines the role of human factors in cybersecurity decision-making, emphasizing Knowledge–Attitude–Behavior (KAB) frameworks and data-driven models. It highlights that while technical standards support compliance, behavioral factors are often insufficiently addressed. The study underscores the importance of integrating behavioral insights with quantitative approaches to improve the effectiveness and adaptability of organizational cybersecurity strategies.
[37] evaluated various information security awareness training methods and their effects on employees' knowledge, attitudes, and behaviors. While all methods were equally effective in improving knowledge, combining multiple training approaches had a stronger impact on attitudes. Text-based and game-based training were found to be most effective in influencing actual behavior. The findings emphasize the value of engaging and diverse training methods to enhance motivation, reduce security fatigue, and strengthen organizational security.
[38] examines the influence of age and education on the relationships within the Knowledge–Attitude–Behavior (KAB) model in the context of information security awareness among employees in Vietnam. Based on survey data from 400 participants, the findings indicate that younger employees are more likely to translate positive attitudes into secure behaviors, while higher education levels enhance the relationship between security knowledge and attitudes. The study underscores the importance of incorporating demographic factors into the design of effective information security training and awareness programs.

[39]Agency using the Knowledge–Attitude–Behavior (KAB) model. Data were gathered from approximately 30 employees through a questionnaire based on the Human Aspects of Information Security Questionnaire (HAIS-Q). The findings indicate a generally satisfactory level of awareness (80.82%), with most indicators rated as good. However, weaker performance was observed in areas such as internet use, social networking, incident reporting, and mobile computing, highlighting the need for targeted training and awareness initiatives to improve employees' security practices.

Based on the literature review conducted on the use of KAB model in information security, the KAB model is mainly used to measure the effectiveness of information security awareness programs. The knowledge component of the KAB model is enhanced to include the elements of e-learning so that the effectiveness of using e-learning can be measured. However, given that there are many different types of security knowledge, it is not yet known which of them can influence the employee's security behavior and in what way the behavior is influenced by the knowledge. This has not been explored in any of the previous research works on the use of KAB model in information security. It is hypothesized that different types of security knowledge will have different influence on an employee's security behavior and therefore the KAB model as proposed by Kruger & Kearney (2006) needs to be extended and adapted to represent the relationship between the security knowledge construct and behavior. In particular, the knowledge component of the KAB model needs to be extended to include the relevant security knowledge constructs that can be included in an information security awareness program so that the impacts of each type of knowledge on the attitude and behavior of the employee can be measured.
In this study, the knowledge–attitude–behavior (KAB) model is extended and adapted to reduce internal security incidents within the framework of information security culture. It can serve as a guide for organizations to instill the security knowledge required among employees to influence their behavior when interacting with information assets, thereby minimizing security risks.

3. KAB Model

In the KAB model [28], as shown in Figure 1, knowledge influences an individual's attitude toward a particular behavior, which in turn enhances the desired behavior. The model highlights the role of knowledge in behavioral change and the accumulation of knowledge, with such accumulation leading to changes in attitude and, ultimately, to changes in behavior. In other words, as knowledge about a certain behavior accumulates, corresponding changes occur in attitude, which

progressively influence the behavior in question.

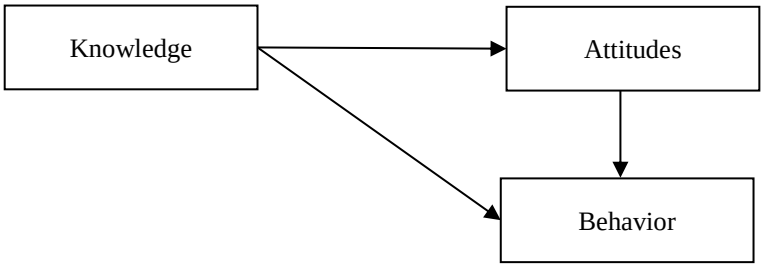

Figure 1. KAB Model

3.1 Relationship between Knowledge, Attitude, and Behavior in the KAB Model

Kruger and Kearney [5] proposed a prototype model grounded in concepts drawn from social psychology, suggesting that individuals develop learned predispositions to respond positively or negatively toward a specific object. These predispositions consist of three main components: affect, behavior, and cognition. Based on these elements, the model was structured around three corresponding dimensions, namely what an individual knows (knowledge), how they feel about a subject (attitude), and how they act (behavior). [29],[41] argued that social psychological principles could be utilized to improve the effectiveness of an information security awareness program.

[28] developed a prototype for measuring information security awareness using KAB. The underlying theory of the KAB model seeks to understand the relationship between these three components, suggesting that as knowledge accumulates in a relevant domain—for example, in information security, health, or education—it eventually initiates changes in attitude, which gradually lead to changes in behavior. In the KAB model [28], as shown in Figure 1, knowledge refers to what an employee knows, attitude focuses on what an employee thinks, and behavior relates to what an employee does [30]-[32].

The KAB model posits that knowledge is accumulated over time within a relevant domain. For instance, in various fields such as information security, health, the environment, or education, this accumulation of knowledge initiates changes in attitude. The model highlights the role of knowledge in behavioral change, showing that knowledge accumulation leads to changes in attitude, and, ultimately, to changes in behavior.

4. Adapted KAB Model

Based on the literature review on the use of the KAB model in information security, the KAB model developed by [28] has been used to represent the relationship between knowledge and behavior. The model is based on three equivalent dimensions: what a person knows (knowledge), how they feel about the topic (attitude), and what they do (behavior) [28].

In this study, the KAB model is adapted by extending the knowledge component to include security knowledge constructs to influence employee behavior. Therefore, as shown in Figure 2, the knowledge dimension is extended to include constructs such as knowledge of security threats, knowledge of security technologies, knowledge of organizational security policies, knowledge of security responsibilities, knowledge of security risks, and knowledge of legislation, regulation, and national culture [42]. The adapted KAB model incorporates these security knowledge constructs to define the relationship between knowledge, attitude, and behavior.

Figure 3 shows the relationship between knowledge, attitude, and behavior in the adapted KAB model. In this model, knowledge influences an individual's attitude toward a particular behavior, which in turn enhances the desired behavior. The model highlights the role of knowledge in behavioral change and its accumulation, with such accumulation leading to changes in attitude and, ultimately, to changes in behavior. In other words, as knowledge about a specific behavior—such as security behavior—accumulates, corresponding changes occur in attitude, progressively influencing behavior. If employees can interpret and understand security policies and relevant documents, they are likely to behave in accordance

with official security guidelines. They can perform security activities accordingly, and their security behaviors become observable. These visible security behaviors are important because they serve as good examples of security practices that can inspire everyone in the organization. Ideally, once employees know how to perform security activities in their daily work routines, security practices can become embedded within the organization, helping to influence behavior and cultivate an appropriate security perception among employees.

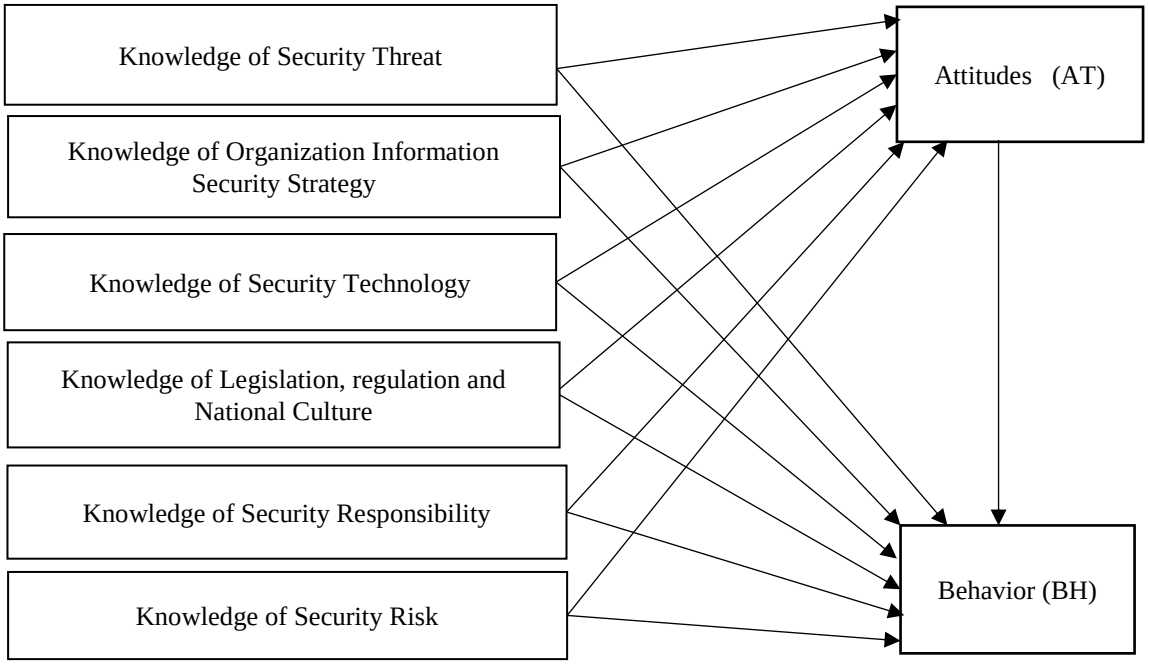

Figure 2. Adapted KAB model

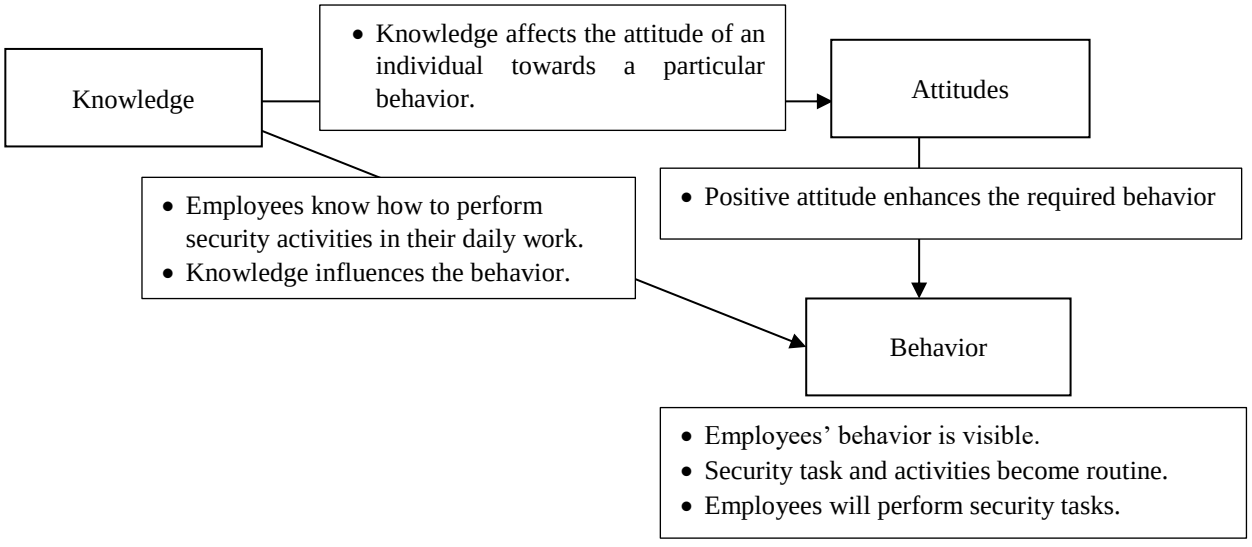

Figure 3. Relationship between knowledge, attitude, and behavior in the adapted KAB model

(A). Variables of the Adapted KAB Model

The KAB model is extended to include relevant knowledge constructs, enabling representation of the relationship between various types of security knowledge and behavior. In this section, the variables of each element in the KAB model—knowledge, attitude, and behavior—are identified and analyzed using content analysis based on the literature review. This approach provides an in-depth understanding of the variables and principles of security knowledge constructs. Table 1 presents the variables associated with each element of the KAB model.

Table 1. Variables of the Adapted KAB Model

Security Knowledge **(Security Knowledge Construct)**	**Attitude** **(Attitude toward Security Knowledge Construct)**	**Behavior** **(Security Behavior)**
-Knowledge of Security Threat -Knowledge of Organization Information Security Strategy -Knowledge of Security Technology -Knowledge of Legislation, Regulation and National Culture -Knowledge of Security Responsibility -Knowledge of Security Risk	- Necessary to know - Important - Benefit - Help to mitigate the risk. - Valuable - Positive effect to protect - Minimize the risk. - Influence behavior - Guide behavior.	- Update antivirus regularly. - Lock computer. - Clear disk policy. - Report security incidents. - What to protect. - What to do. - Share Information - Follow organizational policy. - Prevent, detect, respond, and reflection. - Follow organization security policy. - Manage password regularly. - Protect confidential information. - Do not open attachment from unknown senders.

These variables help provide an in-depth understanding of the elements of knowledge, attitude, and behavior in the KAB model. The model aims to direct the employee behavior and help establish an appropriate security perception among employees to minimize the internal security incidents, reduce the risk of exposure of information assets, and determine the relationships between knowledge, attitude, and behavior.

5. Security Knowledge Required to Improve Employee Behavior

The related studies concerning security knowledge was gathered for systematic review and analysis using qualitative content analysis. Such analysis uses a subjective interpretation of the text content using a systematic process of classification that codes and identifies themes/patterns within the text.
In the following subsections, the security knowledge required to influence the employee behavior are resented. Theses security knowledge needed to be provided to employees in order to enhance their behavior in their interaction with information assets of the organization in order to lessen the risks towards such assets.

4.1 Knowledge of Security Threat

In the world of technology, the threats are innumerable and are of different types and goals, like vandalism, thievery or extortion. There are many forms of cyber-threats, with some common ones taking the forms of, viruses-a set of computer programs that can disturb or slow down the performance of the computer or prevent normal functioning of computer systems or malware – malicious software/program that can harm information systems such as viruses, spyware, trojan horses or worms. Threat has a negative consequence such as loss of data, loss of money and blocking access to information [43]. These threats are often introduced to the organizations via email attachments or programs downloaded from the Internet. It can also come in the form of Spam: an unsolicited e-mail or undesirable email, spyware: monitoring and spy

software, denial of services attacks to make computer resources unavailable to the users, social engineering to obtain a confidential information via interaction or communication with insiders, or phishing to perform a malicious action. The main objectives of these threats may be to steal, monitor, change or expose confidential data or assets related to the users.
Employees inside the organization pose direct or indirect threats to the organizations, with the information assets within vulnerable to cyber-attacks that are more often than not, detrimental to the organizational performance. Thus, the inculcation of security knowledge culture among employees will contribute towards lessening the threats within the organization and protecting its information assets. Organizational employees always have to be aware of threats and to achieve this, security knowledge regarding security threats has to be instilled in them. The organization should provide security knowledge in terms of threats to employees to direct and manage their behavior in their interaction with its assets.

4.2 Knowledge of Organization Information Security Strategy

The organization information security strategy describes the suitable implementation of various information security strategies such as plans of actions, policies, objectives, best practices, standards, guidelines and priorities that guide employees to accomplish goals to safeguard information assets.
Studies in literature have examined the relationship between information security culture and security policies (e.g., [44]-[46]. More specifically,[47] stated that information security policies is an important component of information security culture, while [48] suggested that security policy development needs to be supported by the security culture of the organization.
Added to the above, [49] argued the primary aim of a policy is to drive the decisions, actions and behaviors of employees relating to their interaction with the information assets. Such policy explains employees' acceptable behavior; for example, the information security policy mandates that laptop must be physically secured at all times. The policy statement aims to direct employee behavior towards the protection of physical assets and data saved in the laptop – it aims to influence the behavior of the employee when using the laptop to ensure its safety. The absence of such statement and its enforcement could lead to employees being careless of their laptop's security. In other words, lack of information security component to direct and influence employee behavior could lead to employees leaving information assets at risk. The negative consequences could lead to an unacceptable culture of neglect.
Employees would comply with information security policies and practices if they understand the importance of information security in protecting the valuable assets of the organization against unauthorized and intentional misuse by individuals that violate hardware, software, data and computer services [50]. This can be done via management support, and the provision of information security programs and information security guidelines that are clear. The level of user awareness can be maximized if the whole organization practices the recommended information security, and in turn, this brings about successful implementation of information system security within the organization.
In a similar line of study, [51] related that in case employees are privy to the information security policy, they are more likely to comply with it. Employees primarily focus on their tasks and jobs and may not be aware of the new policy (e.g., new password requirements) but an effective information security culture ensures that they are made aware of it to protect their computers and sensitive information against threats, this way adherence becomes a norm.
In organization, the management must focus on how each statement of the organization's policies, guidelines and strategies has to be positively stated to influence human behavior and to uphold information security culture. The objective has to be geared towards instilling information security behavior that protects information assets based on the information security policies, strategies, guidelines and best practices of the organization. This type of behavior could entail reporting security incidents, compliance with clear desk policy, or secured disposal of confidential documents.
Providing security knowledge about organization information security strategy directs employees' behavior to safeguard information assets, facilitate oversight and determine who has control access. This necessitates the employees' obtaining knowledge on the policy and its positive outcomes directed towards protecting assets as a result of complying with the policy. The objective of policy is to influence and to improve the employees' behavior to ensure the protection of information assets.

4.3 Knowledge of Security Technology

In this paper, knowledge of security technology is knowledge concerning hardware, software, services, appliances and applications employed by the organization for the protection of information assets [26]. Disseminating knowledge concerning security technology has a key role in forming information security culture and in influencing and enhancing employees' behavior towards protecting the organization from within. Stated clearly, creating and maintaining an effective information security culture will facilitate the use of various security technology measures. For instance, the antivirus software would be useless to the organization without its regular update. This holds true for the other security technologies deployed by the company when inappropriately utilized by employees. Developing knowledge of security technology

would thus contribute to urging employees' behavior towards protecting the organizational assets by using available security technology correctly.

Majority of organizations use different technology control for the protection of information security and for the prevention of threats and security attacks; for instance, the use of firewall, antivirus software, access management systems, these are aimed to safeguard the organization from threats and attacks and to support its security strategy. Nevertheless, the lack of sufficient knowledge of employees on policy usage of technology may lead to ineffective use of them and may do more harm than good to the organization. Therefore, providing security knowledge about security technology is a vital to influence the employee behavior inside the organization.

4.4 Knowledge of Legislation, Regulation and National Culture

The organization's external environment and national culture significantly impact its information security culture. According to [52], organizations develop their information security assumption on the basis of their social values reflecting the environment. Stated clearly, the legislation, regulation, and national culture of the environment within which the organization is run have to be considered when designing the organization's structure, its information security culture, and security of information assets (Hogail, 2015).

Several studies have been dedicated to this topic and they focused on external factors that influence the information security culture, including national and cultural factors (e.g., [54], [55], [56]. Several studies, including those referenced in [57], have identified national and ethical culture, as well as governmental legislation, as external factors that can significantly influence information security culture. In addition, the study in [56] emphasizes key determinants such as corporate governance, the legal and regulatory environment, and corporate citizenship. The author further argues that security culture is shaped by organizational culture, which itself is influenced by national culture. The findings demonstrate that corporate governance, legal and regulatory frameworks, and corporate citizenship collectively play a crucial role in shaping an organization's information security culture. n this context, multiple studies in the literature have confirmed the strong impact of national culture on the implementation of information security culture and on employees' behavior[54]-[59]. Moreover, national culture determines the values and beliefs of the members of the organization because it naturally influences the viewpoints of the members, their duties and their interaction – in sum; it defines acceptable and not-acceptable behavior in the organization. This indicates that when information security culture is designed, national culture has to be taken into consideration due to its influence on human behavior. Also, employees should be knowledgeable on legislation, regulation and national culture when it comes to privacy issues and security information laws, as well as intellectual property.

Moving on to legislation, Al Hogail [27] argued that an effective information security culture within an organization can be ensured by taking legislation into account in that government regulations concerning information security has to be applied (e.g., copyrights). It is crucial to inform employees of relevant government information security linked to legislation. On the above studies, it is clear that providing this knowledge to employee help to influence their behavior to protect the organization information assets.

4.5 Knowledge of Security Responsibility

The employees working for the organization is deemed to form the core of its information security culture on account of their important role in protecting information in the information security process [60]-[62]. Information security culture primarily aims to facilitate employees' behavior to work towards the security of information assets, from the top management level to the most menial worker [63]. One of its main goals is to establish that information security is the responsibility of every employee, in that the knowledge of security responsibility culture has to be inculcated in each employee in order to protect the organization from within. Al Hogail in [53] stressed that information security culture has to consider every human factor to enhance user security behavior. In reality, majority of the employees think that the security of information falls on the IT department's responsibility [64], when in fact, employees should be aware of their security related roles and responsibilities and their security behavior (ISO/IEC27001:2013). The concept of knowledge of security responsibility should be established among all employees to have a positive impact on their behavior. The responsibility of top management in this case is to develop security measures for the data protection, to commit towards data protection and information security to promote the desired behavior of employees. The management should also have as strategies to improve information security in the organization [27].

Knowledge of security responsibility has to be disseminated among employees through training and awareness in order to achieve the desired employees' behavior and to improve information security culture [65], [66]. Employees have to be educated of their security related roles and responsibilities and trained to behave in a secure manner. They should know

how to effectively use information security applications and procedures and what is expected from in their interaction with information assets. They should also know what to do when they detect a security breach, how to disclose threats and risks that can potentially harm information assets. In sum, they should know what to protect, why it needs protection and how they be a part of the protection [67].

Conversely, the employees should be made accountable for their actions, these actions should be taken against employees who fail to comply with information security requirements. In relation to this, top management should establish clear policies and formal reward and punitive processes for effective information security culture. Security responsibility culture should be promoted within the organization through reward and deterrence processes and security oversight. There are evidence that have shown that rewarding desirable behavior and punishing undesirable ones would maximize the adherence of employees to information security needs [47], [68].

4.6 Knowledge of Security Risk

Similar to the previous types of knowledge, this is equally important to drive human behavior in their interaction with the organization's information assets and to understand the risks present in the environment of the information assets. In 2018, a security violation survey by PWC (Price Waterhouse Coopers) revealed that 28% of major organizations reported security breaches from within, 57% of small organizations experienced insiders related security violation, and 36% of the breaches stemmed from unintentional human behavior (Information Security Breaches Survey, 2018) (Correct the referencing method). For the establishment of an effective information security culture in the organization, focus should be placed on risks linked with unmanaged behavior. It is crucial to educate employees and alert them on the risks and dangers stemming from the environment that surrounds information assets and the risks that may occur when employees are behaving insecurely within the organization [27].

Knowledge of security risk aims to promote employees' awareness of security risks and their responsibilities towards security that drive them towards acting in a secure way [47], [69]. Additionally, the knowledge can assist employees to know, understand and adopt the required precautions and ensure that they possess the required skills for appropriate actions [70], and for the pursuant of secured behavior.

The careless and ignorant actions of the employees could lead to information security risks involuntarily; for example, if an employee retrieves spam email, opens email attachment with virus, or ignore information security policy on external drive use [57]. Moreover, the negligence of employees could leave the network to risk from malware, virus, worms and Trojans from infiltrating and infecting the whole system. This is also exemplified by employees using their personal devices without the right security protocols, in which case, the risks of exposing the network to security threats and attacks are increased. Authors in [71] stated that many employees carry mobile devices containing sensitive work related information outside their workplace, which could expose sensitive data to the risk of being leaked or stolen. Other behaviors that expose employees and data to security risks include downloading suspicious software, browsing through unsafe websites, sharing passwords, or leaving written passwords at open places in the office such as writing password on a post note and pasting it on the monitor. Inculcating knowledge of security risk to employees will contribute towards safeguarding them, the organization and the information assets of the organization. It will also make them aware of the potential risks, which in turn, would affect their behavior and actions taken in conducting their work.

6. Adapted KAB Model for Internal Information Security Risks

An information security culture develops as a result of employees' information security behavior, in the same way that organizational culture develops from employees' behavior within the organization [9]-[12], [21],[34]. An information security culture is therefore based on employees' interactions with information assets and the security behavior they exhibit within the context of the organizational culture. It can be defined as the attitudes, assumptions, beliefs, values, and knowledge that employees use to interact with the organization's systems and procedures at any given time. These interactions result in either acceptable or unacceptable behavior [73].

Furthermore, employee behavior can be defined as "the way an employee conducts their work, either positively or negatively" [74]. Employee behavior within an organization can significantly affect the effectiveness of the organization's information security.

In [47], the interaction between behavior and information security culture is described through a model. This model illustrates how information security components, such as knowledge of security policies, interact with employees' behavior, ultimately influencing the resulting information security culture, as shown in Figure 4.

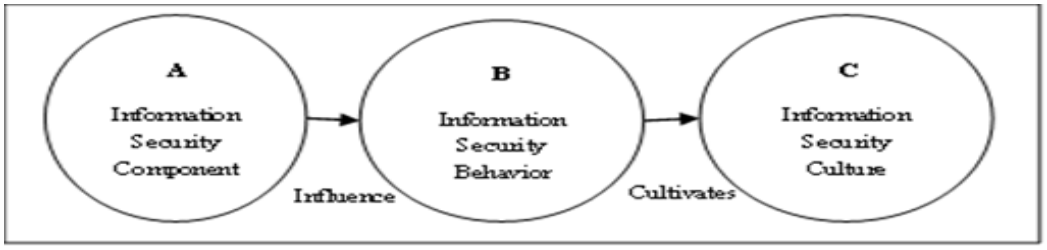

Figure 4. Influence of information security behavior on cultivating an information security culture [47]

Figure 4 illustrates that information security components (Part A in Figure 4) are implemented within the organization. These components act as inputs that influence employees' information security behavior (Part B in Figure 4). The implementation of these components shapes the way employees interact with organizational information assets, ultimately leading to behaviors that are referred to as information security behavior.

The objective is to encourage employees' security behavior in ways that protect information assets, based on the security knowledge constructs in the adapted KAB model. Such behaviors may include reporting security incidents, adhering to a clear desk policy, managing passwords, or securely disposing of confidential documents. Over time, these security behaviors become embedded in daily organizational practices, thereby establishing an information security culture (Part C in Figure 4). A culture is thus promoted where information security is accepted as the standard way of doing things. To illustrate the interaction between parts A, B, and C in Figure 4, consider the implementation of security knowledge constructs in the adapted KAB model presented in Figure 2. For example, knowledge regarding the information security policy, a component of the organization's information security strategy, aims to influence employees' decisions, actions, and behaviors [9], [75]. The policy specifies acceptable and unacceptable behaviors. For instance, it may state that laptops must always be physically secured (Part A in Figure 4). This statement directs employee behavior to protect both physical assets and the data stored on the laptops (Part B in Figure 4). Over time, this behavior becomes standard practice, cultivating an information security culture (Part C in Figure 4). Without such guidance and enforcement, employees could leave laptops unsecured, increasing organizational risk.

To cultivate an effective information security culture, organizations should implement a comprehensive set of security knowledge constructs in the adapted KAB model. These constructs address human, process, and technical threats and help guide employee behavior to establish an appropriate security perception across the organization [4],[12],[39]. Organizations should ensure that employees' interactions align with the requirements of these constructs, such as backing up servers daily, protecting removable media with passwords, or deleting unsolicited emails with attachments. Employees must possess adequate security knowledge concerning their roles and responsibilities, and security knowledge should be reinforced through day-to-day activities, making information security a natural part of daily routines.

When employees have a clear understanding of security policies and related documents, they are more likely to adhere to official guidelines. Their security behaviors become observable, serving as examples that can inspire others. Over time, these behaviors become embedded in the organization's daily routines, helping cultivate an appropriate information security culture. Furthermore, understanding the importance of security knowledge constructs, knowing how to apply them, and knowing where to report incidents can help reduce internal security incidents while enhancing organizational effectiveness and asset protection [75]. Awareness, training, and education programs can improve employees' handling of information and increase accountability for their actions. Organizations should provide training on key security knowledge constructs in the adapted KAB model, including knowledge of security threats, organizational information security strategy, security technology, legislation, regulation, national culture, security responsibilities, and security risks. This training aims to guide employee behavior when interacting with information assets, fostering appropriate security behavior among employees.

According to [40],[41] awareness and training programs are critical success factors in implementing effective information security, significantly improving organizational information security outcomes. Studies [1],[42] emphasize that information security awareness enhances employees' knowledge and behavior, enabling them to apply correct practices and reduce internal security incidents. In study [43],note that awareness programs can positively influence behavior and enhance trust between employers and employees.

The adapted KAB model guides organizations and professionals in influencing employees' behavior by ensuring that employees possess the required security knowledge. The set of security knowledge constructs—knowledge of security threats, organizational information security strategy, security technology, legislation, regulation and national culture, security responsibilities, and security risks—can be categorized (Part A in Figure 4) and implemented at individual, group, or organizational levels. Implementing these constructs influences employee behavior when interacting with information assets (Part B in Figure 4). Over time, as such behaviors become standard practice, an information security culture is established (Part C in Figure 4). When employees understand and adopt these behaviors, they are more likely to practice them consistently. Once embedded in daily routines, these behaviors contribute to the development of a strong information security culture within the organization.

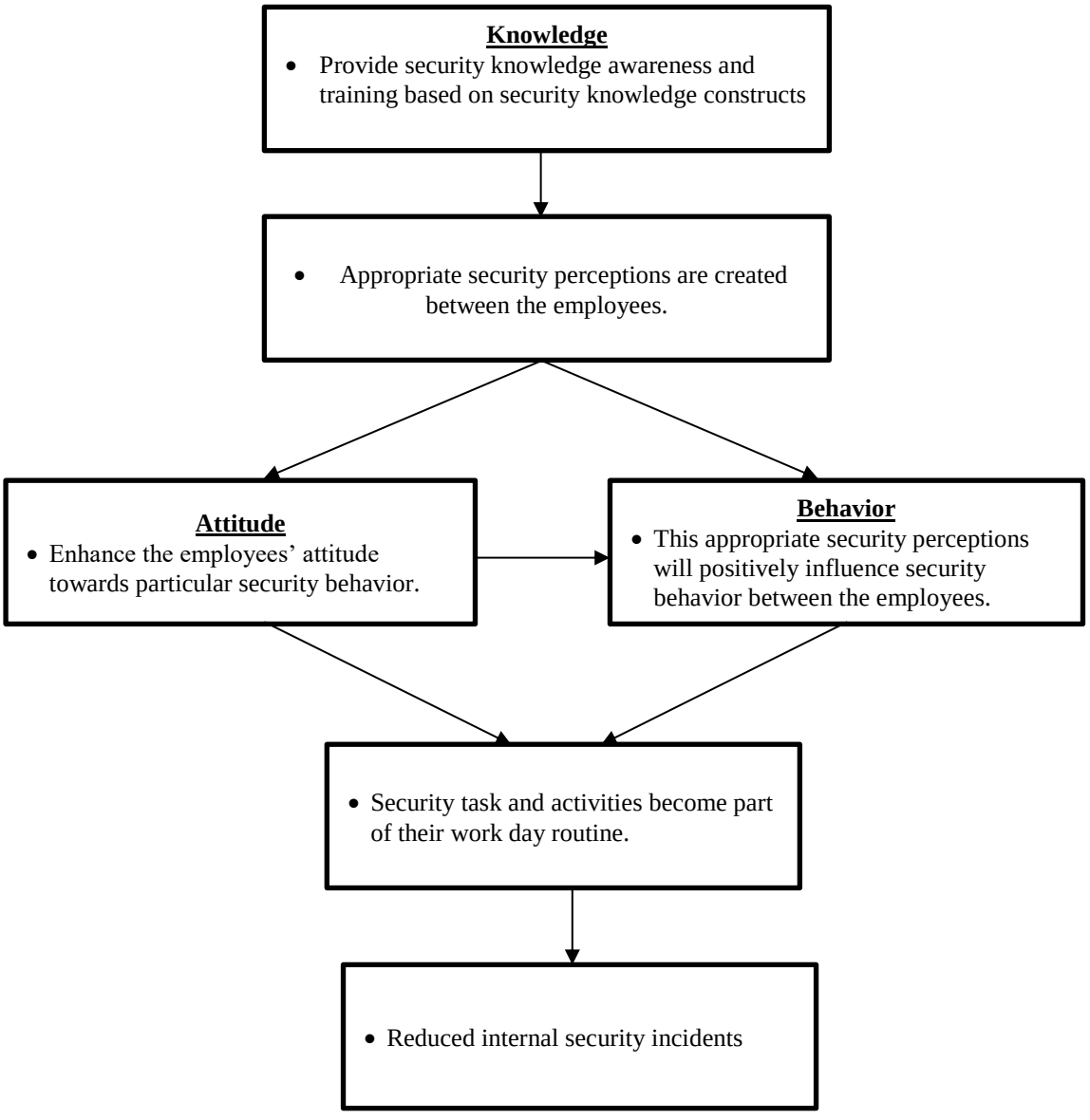

Figure 5. Adapted KAB model for reducing internal security incidents

Figure 5 illustrates the interaction between knowledge, attitude, and behavior in the adapted KAB model presented in Figure 2, which explains how appropriate employee security behavior can be developed to minimize internal security

incidents. As shown in Figure 5, providing employees with adequate security knowledge constructs, awareness, and training helps establish appropriate security perceptions among them. When employees possess a high level of security awareness and demonstrate responsible security behavior, the organization's capacity to safeguard its information assets against internal threats is significantly enhanced. Given that employees routinely handle sensitive information as part of their daily tasks, fostering a strong culture of security awareness and compliance is essential for maintaining the integrity and protection of organizational information assets. These perceptions, in turn, positively influence employees' attitudes and behaviors toward adhering to security practices. Consequently, security-related tasks and activities become part of their daily routines, leading to a reduction in internal security incidents.

Employees, as organizational insiders, recognize the necessity of engaging in specific security practices to ensure the protection of the organization's information assets. Consequently, when employees have the opportunity to perform these tasks as part of their daily work, such practices should become an integral component of their routine activities. Over time, these actions evolve into common practices shared among employees, increasing the likelihood that their behaviors will consistently contribute to safeguarding the organization's information assets. Gradually, the employees' strong commitment to these practices fosters the development of a well-established culture of information security within the organization.

6. Methodology

This study aims to validate the KAB model and to examine the security knowledge constructs required to influence employee behavior within organizations. This is followed by the collection of quantitative data from employees in the healthcare sector.

6.1 Data Gathering by Questionnaire

A questionnaire is a research instrument composed of a set of questions or prompts designed to collect information from respondents [80]. It can be used for exploration, description, or explanation of a case study context[81]. Questionnaire helps the researcher to become more familiar with a phenomenon of interest. [82] suggested the use of questionnaire for data collection on employee's perceptions of actual security behavior in the field of information security culture. The purpose of using questionnaire is to determine the influence of security knowledge constructs on employee behavior in information security culture.

The findings of the study are expected to assist the management to furnish the desired information culture by focusing on security knowledge required that must be inculcated between employees for the enhancement of their behavior. It is pertinent for management to determine suitable techniques for the promotion of awareness and knowledge among employees.

6.2 Questionnaire Development

The security knowledge items required to enhance employee behavior were developed and identified by following guidelines. A cover letter was attached to the questionnaire that explains the researcher and information as well as the objectives of the study to boost respondents' participation in the survey (see Appendix A). The questionnaire had different parts, with each part having its own set of questions, and instructions were provided on the way they should be answered to mitigate ambiguity.

There are nine parts to the questionnaire, with questions about demographic information, security knowledge constructs, attitude and behavior. The first section covered the demographic information, while the remaining eight addressed knowledge of security threat, knowledge of organization information security strategy, knowledge of security technology, knowledge of legislation, regulation and national culture, knowledge of security responsibility, knowledge of security risk, attitudes and behavior. The respondents were requested to tick the relevant answer in front of each item, measured by a 5-point Likert scale. The scale range depicted the following: 1- strongly disagree, 2- disagree, 3- neutral, 4- agree and 5- strongly agree. Likert scale was employed for its easy management, easy answering of questions and high reliability [83]. A 5-point Likert scale was specifically selected as it mitigates the possibility of measurement error and breach of normality in data distribution – in this regard, the Likert scale is a better option against other scales (e.g., Thurstone/Guttman). The used scale is represented in Fig 6 with an example.

Statement	Strongly Agree	Agree	I don't know	Disagree	Strongly Disagree
I update the anti-virus software regularly.					
I always lock my computer when I leave the desk.					

Figure 6. Survey scale example

The questionnaire consists of two parts; the first one contains the demographic details of the participants, requesting their age, year of experience, job level, education level, gender, work in IT department, education background, work requirements, and security awareness. This is followed by the second section that contains items related to security knowledge required to enhance employee behavior and this covers knowledge of security threat, knowledge of organizational information security strategy, knowledge of security technology, knowledge of legislation, regulation and national culture, knowledge of security responsibility and knowledge of security risk. The third section contains behavior, with the attitude construct covered in several questions.

7. Hypothesis Development

This section presents the development of the study hypotheses based on the relevant literature reviewed. Hypothesis testing is used to determine the relationships between the variables of interest, which are central to the study. In this research, the primary focus is on examining the relationships among knowledge, attitude, and behavior within the adapted KAB model.

In this study, the knowledge in KAB model as shown in Figure 2, has been extended to include security knowledge constructs such as knowledge of security threat, knowledge of security technology, knowledge of organization security policy, knowledge of security responsibility, knowledge of security risk, knowledge of legislation, regulation and national culture. The KAB model was adapted to include security knowledge construct to define the relationship between security knowledge constructs, attitudes and behavior, and on this basis, the hypotheses were developed.
On the basis of the above variables, the study hypotheses were developed to determine the impact of security knowledge constructs to employee behavior. The proposed relationships are then tested and confirmed using an organized progression of examination.

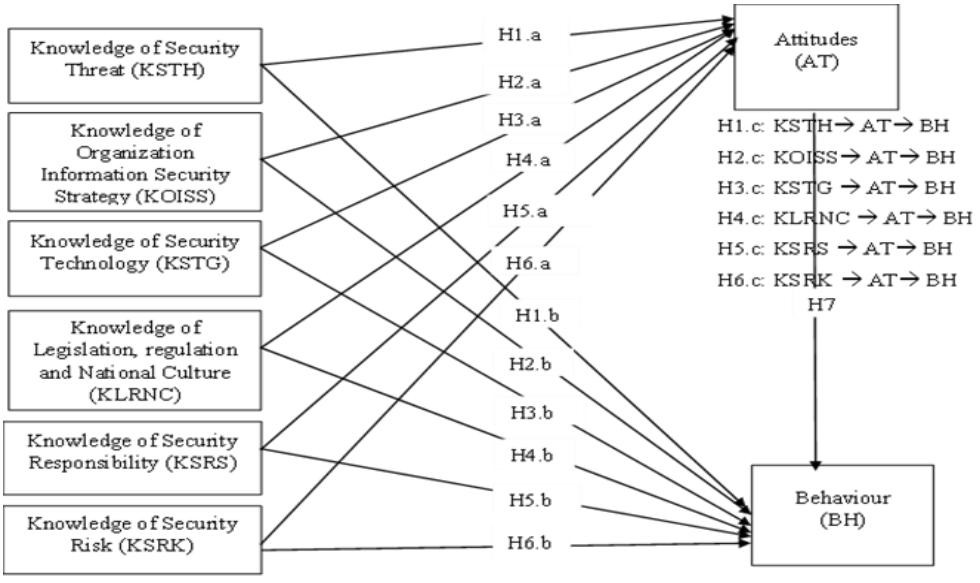

Figure 7. Hypothesis development based on the adapted kab model

7.2 The Relationship Between Knowledge and Behavior

Several studies in literature have been dedicated to studying the knowledge-behavior relationship [37], [38], [77], [84], [85]. The findings showed a positive relationship between security knowledge levels and employees' behavior.
In information security, the human factor comprises of two dimensions and they are knowledge and behavior and both are interconnected [15], [16], [86]. It is crucial for employees to be aware of the importance of information security so that they may safeguard the assets of the organization. In other words, it is crucial for them to understand and apply security knowledge in order to display the right behavior when it comes to the concept. In this regard, knowledge should match behavior in order for the desired behavior to be achieved within the organization. Moreover, security behavior is described as the ability of the employee to adopt the suitable and effective security actions [36]. Behavior is the assumption about what behavior regarding the protection of information is encouraged or not [40].

On the other hand, knowledge refers to the theoretical and practical understanding of the subject, fact, information, value or skill accomplished via education or experience [87]. Knowledge has its basis on user knowledge on the right behavior to adopt in specific situations [88]. It has the ability to increase the required behavior relating to information assets of the organization. On the basis of the ability to know and understand the constructs of security knowledge, it is crucial for the employees to know the security threats in the form of viruses, spam email, downloading suspicious software, phishing issues, scan attachment in emails and access trusted sites. Furthermore, employee must know how to have strong passwords, do not share password between others, and change it constantly based on the policies of the organization. Employee must know and understand security knowledge construct as illustrated in adapted KAB model. Employees having the right knowledge concerning security knowledge constructs are expected to be able to manage behavior and safeguard the information assets of the organization. On the basis of the discussion above, the following hypotheses are formulated, which are depicted in Figure 7.

The knowledge of security threats among the employees in the organization has a positive impact on their behavior and thus the following hypothesis is proposed to be tested;
H1b: There is a significant relationship between knowledge of security threat and behavior.

The knowledge of organizational information security strategy among the employees in the organization has a positive impact on their behavior and thus the following hypothesis is proposed to be tested:
H2b: There is a significant relationship between knowledge of organization information security strategy and behavior.

Moreover, the knowledge concerning the technology among all the employees in the organization has a positive impact on their behavior and thus,
H3b: There is a significant relationship between knowledge of security technology and behavior.

Also, the knowledge concerning legislation, regulation and national culture of all the employees in the organization positively impacts their behavior and thus, the following hypothesis is proposed to be tested;
H4b: There is a significant relationship between knowledge of legislation, regulation and national culture, and behavior.

The employees' knowledge on security responsibility positively impacts their behavior and therefore,
H5b: There is a significant relationship between knowledge of security responsibility and behavior.

Lastly, knowledge of all employees concerning security risk has a positive effect on their behavior and thus, the following hypothesis is proposed;
H6b: There is a significant relationship between knowledge of security risk and behavior.

7.3 The Relationship Between Attitudes and Behavior

The attitude-behavior relationship has been examined with the help of several theories, like the Theory of Planned Behavior (TPB), a theory developed by Ajzen (1991) from the Theory of Reasoned Action (TRA). The TPB focuses on improving the compliance behavior of individuals through their attitudes, perceived behavioral control and subjective norms – these constructs influence the intention of individuals towards a specific behavior [22].
In addition, the attitudes-behavior relationship was extensively studied in literature; for instance,[89] investigated and

analyzed the effect of cultural dimensions on the Saudi information security in the context of the health service. The author based the study's conceptual framework on the theory of human behavior, with the attitude of the individual being the major element of his behavior. The Human Behavior theory posits that the individual's attitude is the major component forming his intention to behavior and his actual behavior.

In a study presented by [90], assessed information security attitudes among university students, focusing on participants' attitudes towards accidental information security behavior among university students. Their theoretical framework was based on Ajzen's theory of planned behavior (TPB). They recommended further studies to understand the employees' attitudes towards behaviors. Also,[36] focused on the underpinning behavioral contexts of information security in the workplace, and explored the way individual and organizational factors influence the interactions of the motivations and barriers of security behaviors. The analysis findings showed a positive relationship between attitudes and behavior and a positive relationship between knowledge and behavior.

Employee behavior can change based on one's attitude. Behavior that is liked or disliked, desirable or undesirable, good or bad, or behavior that is viewed positively or negatively [20]. Many studies support the relation between attitudes and behavior. This suggests that attitude may be an important antecedent of security behavior. This context shows that the attitudes of employees on knowledge and understanding the constructs of security knowledge required positively impacts their behavior. On this basis, the study proposes the related hypotheses based on Figure 7.
The attitude of employees towards security knowledge required in the organization positively impacts their behavior and thus;

H7: Employees' attitude towards security knowledge required has a positive effect on their behavior.

7.4 The Relationship Between Knowledge and Attitudes

In this section many definitions of attitude is presented, such as; attitude is described as the positive or negative feeling towards a given behavior and it is defined as the learned inclination to evaluate things in a certain way [91]. Such evaluation may be positive or negative regarding an object, issue, people or events [92]. Attitude stems from the past and present of the individual and it is often related to as the evaluation of objects, people, activities, events and ideas ranging from extremely positive to extremely negative. It is also described as the individual's positive or negative view concerning his engagement with a specific behavior. According to [93], attitude is a psychological inclination that ranges from extremely negative to extremely positive ends. The attitude concept has attracted the attention of many experts in the different domain, because of its potential to describe an individual's behavior.

Majority of studies revealed the existence of knowledge-attitude relationship [16], [78], [94], [95]. Some authors found a significant relationship, whereas others indicated a moderate one. To protect critical information assets, promoting a campaign on security education assists in modeling attitudes and behaviors of managers and employees [96]. Knowledgeable employees who are privy to the security knowledge constructs tend to have a positive attitude towards safeguarding the information assets of the organization. Hence, the following hypothesis is proposed as presented in Figure 7.
Security threat knowledge of the employees within the organization has a positive impact on their attitude and therefore;

H1a: There is a significant relationship between knowledge of security among employees and their attitudes.

Knowledge concerning information security strategy of all the employees of the organization has a positive impact on their attitude and therefore;

H2a: There is a significant relationship between knowledge of information security strategy of employees and their attitudes.

Moreover, knowledge of employee concerning security technology has a positive impact on their attitude and therefore, the following hypothesis is proposed;

H3a: There is a significant relationship between knowledge of security technology of employees and their attitudes.

Furthermore, the employees' knowledge of legislation, regulations and national culture has a positive impact on their

attitude and thus, the following hypothesis is proposed to be tested;

H4a: There is a significant relationship between knowledge of legislation, regulation and national culture among employees and their attitudes.

Along a similar line of hypothesis development concerning knowledge of security responsibility among employees, such knowledge has a positive impact on employees' attitude, which leads to the following hypothesis;

H5a: There is a significant relationship between knowledge of security responsibility among employees and their attitudes.

Also, knowledge of security risk among all employees has a positive impact on their attitude. Therefore, it is hypothesized that;

*H6a: There is a significant relationship between knowledge of security risk among employees and their attitudes***.**

7.5 Relation Between Knowledge, Attitude and Behavior

When employees are provided with knowledge concerning security knowledge, this would work towards transforming their attitudes, assumptions, views and knowledge and will impact their behavior in the organization [7], [40], [97], [98].

In fact, several studies have been dedicated to examining the knowledge-attitude-behavior relationship. More specifically, [99] assessed and measured the effectiveness of information security awareness initiative using KAB model. He found that such initiatives influence and enhance the knowledge, attitude and behavior of users towards information security. Generally speaking, information security awareness companions positively impact the actual working environment of employees in terms of their knowledge, attitude and behavior.

In a related study, der Linden, 2012 looked into the area of climate change and indicated ample evidence to support a significant environmental knowledge-attitudes-behaviors relationship. Meanwhile, a study conducted by [39] employed the KAB model to evaluate the effectiveness of security awareness training. The study revealed a positive relationship among the three aforementioned constructs.

Similarly, a small-to-moderate positive relationship was reported between organizational information security culture and aspects of employees' information security decision-making by [90]. In other words, organizations possessing optimum information security culture had a higher tendency for employees to have knowledge, attitudes, and behavior that is aligned with the information security policies and procedures. This indicates that enhancing the security knowledge could improve adherence of employees to policy and procedures and minimize human-based cyber risks.

More importantly, the employees' security knowledge construct assumed to have a positive indirect impact on their behavior via attitude, where attitude mediates the relationship between security knowledge constructs and behavior. Thus, the employees' knowledge on security threat is assumed to have a positive indirect impact on their behavior via attitude, where attitude mediates the relationship between knowledge of security threat and behavior. Therefore, as presented in Figure 7, the following relationship is hypothesized:

H1c: Attitudes (AT) of employees mediate the relationship between their knowledge of security threat (KSTH) and their behavior (BH).

In relation to the above hypothesis, the knowledge of organization's information security strategy among employees is assumed to positively and indirectly impact on their behavior via attitude. Stated clearly, attitude is hypothesized to mediate the relationship between knowledge of organization information security strategy and employees' behavior, which leads to proposing the following hypothesis;

H2c: Attitudes (AT) among employees mediate the relationship between their knowledge of organization information security strategy (KOISS) and their behavior (BH).

This holds the same for the knowledge of security technology among employees and the presence of its positive and indirect impact on employee behavior via attitude. Attitude mediates the relationship between knowledge of security technology and behavior and therefore, this study proposes the following hypothesis for testing;

H3c: Attitudes (AT) among employees mediate the relationship between their knowledge of security technology (KSTG) and their behavior (BH).

Moreover, knowledge of employees of legislation, regulation and national culture of the organization positively and indirectly influences their behavior via attitude. In other words, attitude mediates the relationship between knowledge

among employees concerning legislation, regulation and national culture and their behavior. Therefore, the following hypothesis is proposed to be tested;

H4c: Attitudes (AT) among employees mediate the relationship between their knowledge of legislation, regulation and national culture (KLRNC) and their behavior (BH).

Furthermore, employees' knowledge on their security responsibility in the organization has a positive and indirect impact on their behavior through attitude, where attitude mediates the relationship between the first two constructs. Therefore, the following hypothesis is proposed to be tested;

H5c: Attitudes (AT) among employees mediate the relationship between their knowledge of security responsibility (KSRS) and their behavior (BH).

Finally, the employees' knowledge on security risk positively and indirectly impacts their behavior through attitude, where attitude mediates the relationship between the former two. Thus, the following hypothesis is proposed to be tested.

8. Results and Analysis

The research objectives and hypotheses served as a basis for selecting the most appropriate methods for analyzing the data collected from the surveys. The survey data were analyzed using Analysis of Moment Structures (AMOS) version 20, along with the Statistical Package for the Social Sciences (SPSS) version 18. AMOS was chosen as a covariance-based Structural Equation Modeling (SEM) tool due to the availability of sufficient theoretical support and the relative simplicity of the proposed model.

(A). Reliability

Cronbach's alpha is one of the most widely used techniques for assessing reliability by providing an indication of internal consistency Cronbach's alpha [100]. In this study, Cronbach's alpha values for each dimension and sub-dimension of the framework were analyzed to establish the reliability of the measurement instrument. The acceptable threshold for Cronbach's alpha is a minimum value of 0.60 to ensure the consistency and reliability of the model. The results of the reliability analysis are presented in Table 2.

TABLE 2. Results of Reliability Test from Pilot Study

1st Order Constructs	**Item number (70)**	**Internal reliability (Cronbach Alpha)**
Knowledge of Security Threat (KSTH)	5	0.855
Knowledge of Organization Information Security Strategy (KOISS)	13	0.919
Knowledge of Security Technology (KSTG)	5	0.893
Knowledge of Legislation, Regulation and National Culture (KLRNC)	9	0.845
Knowledge of Security Responsibility (KSRS)	9	0.913
Knowledge of Security Risk (KSRK)	7	0.844
Behaviour (BH)	15	0.901
Attitudes (AT)	7	0.909

From the table, it is evident that the reliability of the constructs differed from 0.844 to 0.919 and they all exceeded the cut-off value of 0.70 [101]. Evidently, the results met the required Cronbach's alpha (0.70 and over) and thus, reliability was confirmed (Hair, Black, Babin & Anderson, 2010; Sekaran, 2016).

(B). Validity

In order to establish the validity of the proposed model, Structural Equation Modeling (SEM) analysis using the Goodness of Fit Index (GFI) Goodness of Fit Index (GFI) was employed to assess the model fit of the KAB framework. The GFI

criteria indicate that values between 0.90 and 0.94 represent an acceptable fit, while values between 0.95 and 1.00 indicate a good fit. Values below 0.90 are still considered acceptable in some cases [102]- [103]. The results of the goodness-of-fit indices for the measurement model are presented in Table 3.

TABLE 3. GOF Indices of Modified Measurement Model

Fit index	Modified model	Recommended values	Acceptable values
GFI	0.836	≥ 0.90	≥ 0.80

The results have given the indication of the value of GFI was 0.836, which is less than the recommended value of 0.9, but it is still was at a marginal acceptance level and relatively close to the preferred value. [102] argued that value of GFI less than 0.9 does not necessarily mean that the model has a poor fit. [103], [104] stated that GFI values ranging between 0.8 and 0.9 indicate an acceptable model fit. After adjusting for the degrees of freedom relative to the number of variables, the Adjusted Goodness of Fit Index (AGFI) was found to be 0.819, which exceeds the recommended cut-off value of 0.80 as suggested by Chau & Hu (2001) technology acceptance model study.

9. Result and Analysis of Adapted KAB model Hypothesis

This section discusses about the relationship between knowledge, attitude and behavior as discovered from the survey.

(A). DIRECT EFFECTS OF CONSTRUCTS

In the adapted KAB model, the direct effects of Knowledge of Security Threat (KSTH), Knowledge of Organization Information Security Strategy (KOISS), Knowledge of Security Technology (KSTG), Knowledge of Legislation, Regulation and National Culture (KLRNC), Knowledge of Security Responsibility (KSRS) and Knowledge of Security Risk (KSRK) as independent variables on Attitudes (AT) and Behavior (BH) as dependent variables were examined (i.e., H1.a, H2.a, H3.a, H4.a, H5.a, H6.a, H1.b, H2.b, H3.b, H4.b, H5.b, and H6.b respectively). The model also examined the direct effect of Attitudes (AT) on Behavior (BH) (i.e., H7).

The value of R2 for Attitudes (AT) and Behavior (BH) was 0.40 and 0.31 respectively. This indicates, for example, the error variance of Behavior (BH) is approximately 69 percent of the variance of Behavior (BH) itself. In other word, 31 percent of variations in Behavior (BH) are explained by its seven predictors (i.e., KSTH, KOISS, KSTG, KLRNC, KSRS, KSRK and AT). Overall, the findings showed that the R^2 value met the required threshold of 0.30 in the structural equation modeling analysis. Subsequently, the estimated path coefficients were examined to assess the hypothesized direct effects of the variables. The path coefficients, together with the results of the hypothesized direct effects, are presented in Table 4. As shown in table 4, six paths from Knowledge of Security Threat (KSTH), Knowledge of Organization Information Security Strategy (KOISS), Knowledge of Security Technology (KSTG), Knowledge of Legislation, Regulation and National Culture (KLRNC), Knowledge of Security Responsibility (KSRS) and Knowledge of Security Risk (KSRK) on Attitudes (AT) as well as five paths from Knowledge of Security Threat (KSTH), Knowledge of Legislation, Regulation and National Culture (KLRNC), Knowledge of Security Responsibility (KSRS) and Knowledge of Security Risk (KSRK) and Attitudes (AT) on Behavior (BH) were positively significant as their p-values were all below the standard significance level of 0.05. Thus, the hypotheses H1.a, H2.a, H3.a, H4.a, H5.a, H6.a, H1.b, H4.b, H5.b, H6.b and H7 were supported.

Table 4. Examining Results of Hypothesized Direct Effects of the Constructs

Path	Unstandardized Estimate		Standardised Estimate	critical ration (c.r.)	P-value	Hypothesis result
	Estimate	S.E.	Beta			
KSTH → AT	0.142	0.053	0.137**	2.697	0.007	H1.a) Supported

KOISS → AT	0.142	0.063	0.129*	2.268	0.023	H2.a) Supported
KSTG → AT	0.19	0.074	0.165*	2.572	0.01	H3.a) Supported
KLRNC → AT	0.19	0.084	0.150*	2.272	0.023	H4.a) Supported
KSRS → AT	0.241	0.083	0.179**	2.899	0.004	H5.a) Supported
KSRK → AT	0.165	0.068	0.145*	2.424	0.015	H6.a) Supported
KSTH → BH	0.082	0.039	0.114*	2.112	0.035	H1.b) Supported
KOISS → BH	0.01	0.046	0.013	0.217	0.828	H2.b)Not Supported
KSTG → BH	0.031	0.054	0.039	0.576	0.565	H3.b)Not Supported
KLRNC → BH	0.129	0.062	0.146*	2.099	0.036	H4.b) Supported
KSRS → BH	0.136	0.062	0.144*	2.211	0.027	H5.b) Supported
KSRK → BH	0.121	0.05	0.151*	2.405	0.016	H6.b) Supported
AT → BH	0.122	0.047	0.174*	2.593	0.01	H7) Supported

(B). Mediation Effects of Attitudes (AT)

The mediation analysis was used to determine the mediation effects of Attitudes (AT) as mediating variable on the effects of Knowledge of Security Threat (KSTH), Knowledge of Organization Information Security Strategy (KOISS), Knowledge of Security Technology (KSTG), Knowledge of Legislation, Regulation and National Culture (KLRNC), Knowledge of Security Responsibility (KSRS) and Knowledge of Security Risk (KSRK) as independent variables on Behavior (BH) as the dependent variable (i.e., H1.c, H2.c, H3.c, H4.c, H5.c and H6.c respectively). Furthermore, the indirect effects of the independent variables on the dependent variable, mediated by the mediating variable, were also examined. The statistical basis of mediation analysis is correlation. [105]mediation analysis framework proposed a decision-tree approach for testing covariance relationships among three variables: an independent variable (IV), a potential mediating variable (M), and a dependent variable (DV).

The SEM technique is claimed to be preferable to regression techniques for testing mediation because SEM permit modelling of both measurement and structural relationships and yield overall fit indices [106].

The significance of the regression coefficients between Knowledge of Security Threat (KSTH), Knowledge of Organization Information Security Strategy (KOISS), Knowledge of Security Technology (KSTG), Knowledge of Legislation, Regulation and National Culture (KLRNC), Knowledge of Security Responsibility (KSRS) and Knowledge of Security Risk (KSRK) as IVs, Attitudes (AT) as M and Behavior (BH) as DV were examined to determine the occurrence of the mediation effect and its mediating degree. Thus, four hypotheses (i.e., H1.c, H2.c, H3.c, H4.c, H5.c and H6.c) were examined in this section. The results of examining these hypotheses are displayed in Table 5 with the standardized effects of different paths.

As shown in table 5, Attitudes (AT) mediates the effects of Knowledge of Security Threat (KSTH), Knowledge of Legislation, Regulation and National Culture (KLRNC), Knowledge of Security Responsibility (KSRS) and Knowledge of Security Risk (KSRK) on Behavior (BH). Thus, hypotheses H1.c, H4.c, H5.c and H6.c were supported.

Table 5. Results of Examining Mediation Effects of Attitudes (AT)

DV = Behaviour (BH)	**Independent Variables (IVs)**					
	KSTH	**KOISS**	**KSTG**	**KLRNC**	**KSRS**	**KSRK**
Total Effect of IV on DV without M (path c)	0.137**(sig:0.003)	0.035(sig:0.489)	0.067(sig:0.317)	0.172*(sig:0.011)	0.175**(sig:0.006)	0.176**(sig:0.005)
Direct Effect of IV on DV with M (path c')	0.114*(sig:0.013)	0.013(sig:0.737)	0.039 (sig:0.588)	0.146*(sig:0.043)	0.144*(sig:0.026)	0.151*(sig:0.014)
Indirect Effect of IV on DV through M (path b a)	0.024**(sig:0.002)	0.022*(sig:0.010)	0.029**(sig:0.011)	0.026**(sig:0.009)	0.031**(sig:0.005)	0.025*(sig:0.012)
Effect of IV on M (path b)	0.137**(sig:0.002)	0.129*(sig:0.019)	0.165*(sig:0.014)	0.150*(sig:0.014)	0.179**(sig:0.005)	0.145*(sig:0.017)
Effect of M on DV (path c)	0.174**(sig:0.004)	0.174**(sig:0.004)	0.174**(sig:0.004)	0.174**(sig:0.004)	0.174**(sig:0.004)	0.174**(sig:0.004)
Mediation Path	KSTH→AT →BH	KOISS→ AT→BH	KSTG→A T→BH	KLRNC→ AT→BH	KSRS→AT →BH	KSRK→AT →BH
Mediation Effect	Yes	No	No	Yes	Yes	Yes
Degree of Mediation	Partial	---	---	Partial	Partial	Partial
Hypothesis	H1.c)	H2.c)	H3.c)	H4.c)	H5.c)	H6.c)
Result	Supported	Rejected	Rejected	Supported	Supported	Supported

10. Discussion on Hypothesis Testing

This study employed SEM for hypotheses testing, where the proposed research hypotheses were confirmed or rejected.

(A). Relationship between Security Knowledge Constructs and Attitude

Table 4 lists the support for the above hypotheses in the model. To conclude, statistically, there is a significant relationship between security knowledge constructs and attitude, indicating that when security knowledge constructs are instilled between organization employees, their attitude is enhanced and strengthened.

Furthermore, the provision of security knowledge constructs to all employees will positively affect their attitudes concerning the knowledge of security threat, knowledge of organization information security strategy, knowledge of their security responsibility, knowledge of security risks around them, knowledge of legislation, regulation and national culture, and knowledge of security technology. Consequently, such provision will change their attitudes to be more understanding and aware. This result matches those reported by studies in prior literature (e.g.,[107]-[109]. Additionally, to protect

confidential information assets, security education initiatives should be established to assist in changing the attitudes of managers and employees [79]. Hence, extensive degrees of security knowledge constructs inculcated to all employees are related to their improved attitude in protecting the information assets of the organization.

This indicates that when management encourages and promotes awareness training program and knowledge concerning security knowledge constructs, this will support and modify employees' attitudes as a human firewall to safeguard the internal assets of the organization. This is consistent with the interviewee of security experts that sated on the role of enhancing and changing the attitudes of employees. It is crucial for employees to know and understand why they can do and cannot do certain activities. As a result, providing security knowledge constructs to the employees will positively affect their attitudes to protect the organization assets. It is ineffective for individuals to possess knowledge without adopting an appropriate attitude toward information security. Such a situation may lead to ineffective information security practices and increase the likelihood of internal security incidents within organizations. Therefore, it is essential to emphasize the importance of developing the correct attitude toward information security within security education and training program.

On the basis of the present study's findings, it is recommended that the management of organizations should take the importance of security knowledge constructs into consideration to influence and enhance the employee attitudes toward the protection of organization assets from inside. The benefits and opportunities can be determined through a pre- and post-application comparison.

(B). Relationship between Security Knowledge Constructs and Behavior

The relationship results between security knowledge constructs and behavior were presented. It was evident that hypotheses H1b, H4b, H5b, and H6b were all supported. More specifically, the above hypotheses proposed significant effects of knowledge security threat (KSTH) on behavior (BH), knowledge of legislation, regulation and national culture (KLRNC) on behavior (BH), and knowledge of security risk (KSRK) on behavior (BH). Table 4 confirms the support for H1b, H4b, H5b, and H6b in the model. This result supports other results in literature by [110], [111] . However, hypotheses H2b and H3b were rejected as no statistical significant relationships were found between knowledge of organization information security strategy (KOISS) and behavior as well as knowledge of security technology (KSTG) and behavior respectively.

Prior studies in literature revealed that knowledge alone is not the sole drivers of behavior and these include [112], [113] They explained that more than one variable influence behavior. Experts' feedback in the interviews that laid emphasis on security knowledge's role in enhancing and changing employees' behavior. Moreover, the employees have to be aware and understand why they have to follow the organization information security strategy of what they can and cannot do. This supports the adoption of the KAB model in this study, where attitude is considered to have a mediating role in the knowledge-behavior relationship. Based on the result of this study, the relationship between knowledge of organization information security strategy and knowledge of security technology had a significant indirect positive effect on behavior through attitude.

The rejection of hypotheses H2b and H3b may be attributed to the low knowledge of employees regarding the organization's information security strategy, and security technology brought about by the complex security technology and the dynamic nature of technology in terms of hardware and software. Based on the above, healthcare organization as such part of organizations in Palestine lack to security technologies that help to protect the information, lack for security strategies, policies, actions or guidelines to protect the organization information asset, and lack for appropriate security infrastructure to protect the organization information assets. Therefore, there are no significant relationship between the employee's knowledge about security technology and employee's knowledge about organization information security strategy to influence the employee behavior as a case in healthcare organization. So these hypotheses were rejected.

In other hand, the hypotheses H1b, H4b, H5b, and H6b indicate there are significant effects on behavior namely, knowledge security threat (KSTH) on behavior (BH), knowledge of legislation, regulation and national culture (KLRNC) on behavior (BH), knowledge of security risk (KSRK) on behavior (BH), and knowledge of security responsibility (KSRS) on behavior. To clarify, the increase wide use of internet in Palestine and its use to manage the works and tasks within organizations, also the wide use of smart devices among the employees within organization for personal use or for organizational work use. This leads the employee to know about many security risks such as; threats, spyware, extortion, malicious code, phishing, hacking, etc., as a result from using the new technologies in organizations.
The increase of security incidents in organizations and cybercrime lead the employee to become more aware and knowledge

about the risks related to data protection and knowledge about the laws and regulations to data protection act. They also will be more knowledge about their responsibility toward protection of organization asset and their personal data. This security knowledge has a significant impact on employee security behavior towards the protection of organization information assets. Every employee in organization need to know about these security knowledge in order to protect their organization assets. Therefore, understanding and applying security knowledge construct is vital. This implies that, employees must have an appropriate behavior and attitude towards information security. Knowledge and behavior should be in line so that the effectiveness of information security in organization will be achieved.

(C). Relationship between Attitudes and Behavior

The result of the tested attitude-behavior relationship was presented, involving hypothesis H7 that proposed attitude has significant *effect on behavior. The* model supported this hypothesis as evident from the values in Table 4. More specifically, statistically, a significant relationship exists between attitude and behavior. That indicates the higher of employee's attitude towards security knowledge constructs, more positive behavior would be. This result is aligned with those reported by prior studies such as [38], [39], [90] .

Instilling an appropriate attitude toward security knowledge constructs enhances the effectiveness of information security and contributes to reducing internal security incidents within organizations. Therefore, it is essential to emphasize the importance of fostering the desired attitudes among employees toward security knowledge constructs in order to positively influence and improve employee behavior. Based on the hypothesis results, it is recommended that owners and managers of healthcare sector organizations pay close attention to employees' attitudes toward security knowledge constructs, including threats, organizational information security strategy, security technology, legislation and regulations, national culture, security responsibility, and security risk. Addressing these aspects can help positively influence employee behavior and strengthen overall information security practices.

(D). Relationship between Security Knowledge Constructs, Attitude and Behavior

It is evident that hypotheses H1c, H4c, H5c and H6c were supported. Specifically, the mentioned hypotheses proposed the mediating role of attitudes (AT) on the relationship between security knowledge's construct and behavior such as attitudes mediating role on the relationship between knowledge of security threat (KSTH) and behavior (BH), attitudes mediating role on the relationship between knowledge of legislation, regulation and national culture (KLRNC) and behavior (BH), attitudes mediating role on the relationship between knowledge of security responsibility (KSRS) and behavior (BH), and attitudes mediating role between the relationship of knowledge of security risk (KSRK) and behavior (BH). Table 5 shows the support for these hypotheses in the study model. Added to this, the statistical results obtained confirmed a significant relationship between these security knowledge constructs and behavior, with attitude as the mediating variable. Stated clearly, attitude (AT) partially mediated the relationship between security knowledge constructs (KSTH, KLRNC, KSRS and KSRK) and behavior. Furthermore, the results revealed that the knowledge of security threat (KSTH), knowledge of legislation, regulation and national culture (KLRNC) and knowledge of security risk (KSRK) had a significant indirect positive effect on behavior (BH) through attitudes (AT).

Furthermore, the result also indicated that the Attitudes (AT) cannot mediate the relationship between knowledge of organization information security strategy (KOISS) and knowledge of security technology (KSTG)) to behavior (BH). However, the knowledge of organization information security strategy (KOISS) and knowledge of security technology (KSTG) had a significant indirect positive effect on behavior through attitudes.
The above results imply that inculcating security knowledge constructs on employees will positively impact their attitudes towards them, which in turn, lead to a positive impact on their behavior. This result matches with those reported in prior literature, for example, [79], [114], [115], [116], [117].

The examination and testing of the proposed hypothesis show the importance of attitude between the security knowledge constructs and behavior. That means there are a significant indirect positive effect between the security knowledge's (KSTH, KOISS, KSTG, KSRK, KLRNC and KSRS) and behavior. This increase that the organizations have to focus on attitude of employees to perform the desired behavior. Therefore, this study recommends that owners/managers of organizations to consider the importance of attitude in mediating the relationship between security knowledge constructs and behavior among employees, and the indirect positive effect relationship through the attitudes. Promoting security knowledge awareness among employees should be practiced regularly as this will strengthen their attitudes and improve their behavior when interacting with the information assets of the organization. Thus, awareness of security knowledge should be promoted. This assumption matches the feedback provided by the interviewed experts who stressed on the

importance of enhancing security knowledge to change the attitudes and then behavior of employees. Furthermore, critical information assets of the organization have to be protected by launching security education campaign as this would change the attitude and behavior of managers and employees [37], [39], [96]

11. Conclusion

This study aimed to adapt the KAB model to reduce internal security threats within organizations. The findings, supported by a comprehensive literature review, highlight a significant relationship between human knowledge and behavior, and emphasize the importance of identifying the required security knowledge to improve employee behavior. The study also confirms the interrelationship between information security culture and organizational culture, as well as the influence of security culture on employee behavior.

The results demonstrate that security knowledge plays a crucial role in shaping employee behavior when interacting with organizational information assets. Furthermore, the interaction between security knowledge constructs, attitudes, and behavior within the adapted KAB model illustrates its potential effectiveness in minimizing internal security incidents.

In addition, this study identifies key security knowledge constructs that influence employee behavior and provides guidance for organizations to develop appropriate knowledge among employees. This helps in fostering secure behavior and reducing information security risks. The study also addresses gaps in previous research by enhancing understanding of how knowledge constructs contribute to improving behavior within information security culture, thereby supporting managers and organizations in strengthening their security practices.

Finally, the study emphasizes the importance of integrating knowledge, attitude, and behavior through continuous training and awareness programs. Knowledge alone is insufficient without a corresponding positive attitude toward information security. Therefore, organizations must prioritize security education and training to ensure effective employee behavior and to reduce the likelihood of internal security incidents.

Corresponding author
Amjad Mahfuth
Amahfouth99@gmail.com

Acknowledgements
Not applicable.

Funding
No funding

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication
Not applicable.

Competing interests
All authors declare no competing interests

References

[1] S. Skinner, R. Von Solms, … J. van N.-P. C., and undefined 2025, "Cultivating Cybersecurity Awareness Among Seafarers," *Elsevier*, Accessed: Oct. 22, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050925020800

[2] Verizon, "2014 Data Breach Investigations Report," *Verizon Business Journal*, vol. 2014, no. 1, pp. 1–60, 2014.

[3] P. Bhatt, R. Valecha, H. R.-I. J. of Information, and undefined 2025, "Situational awareness about data breaches and ransomware attacks: A multi-dimensional cyber threat impact framework and content analyses of practitioner-public," *Elsevier*, Accessed: Oct. 22, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0268401225000349

[4] V. Marvik and R. Bakir, "Information security culture: An investigation into the impact of a large-scale cyberattack," University of Agder, 2023.

[5] Symantec, "Internet Security Threat Report," vol. 23, no. March, 2018.

[6] A. Mahfuth, "A Systematic Literature Review : Information Security Culture," pp. 1–6, 2017.

[7] N. Alsuqayh, A. Mirza, and A. Alhogail, "A Phishing Website Detection System Based on Hybrid Feature Engineering with SHAP Explainable Artificial Intelligence Technique," *Springer*, vol. 15463 LNCS, pp. 3–17, 2025, doi: 10.1007/978-981-96-1483-7_1.

[8] K. Chauhan, "Insider Threats Mitigation: Role of Penetration Testing," Jul. 2024, Accessed: Oct. 26, 2025. [Online]. Available: https://arxiv.org/pdf/2407.17346

[9] M. Sharulnizam Kamarulzaman, S. Mohamed Shuhidan, K. Abdul Wahid, A. Abdul Wahab, and A. Jalil Toha, "The Current State of Information Security Policies," *istes.org*, vol. 14, no. 1, 2024, Accessed: Oct. 27, 2025. [Online]. Available: https://www.istes.org/storage/01JGK7MF50AKKKW35SCK14TVZW.pdf#page=8

[10] A. D. V.- Diversity, undefined AI, and S. for F. Growth, and undefined 2025, "Encouraging Creativity and Innovation in the Cybersecurity Culture of the Organisation for Sustainable Value and Growth," *igi-global.com*, Accessed: Oct. 27, 2025. [Online]. Available: https://www.igi-global.com/chapter/encouraging-creativity-and-innovation-in-the-cybersecurity-culture-of-the-organisation-for-sustainable-value-and-growth/369102

[11] A. Mahfuth, S. Yussof, A. A. Baker, and N. Ali, "A systematic literature review: Information security culture," in *International Conference on Research and Innovation in Information Systems, ICRIIS*, 2017. doi: 10.1109/ICRIIS.2017.8002442.

[12] H. Zangana, Z. Sallow, M. O.-J. I. Computer, and undefined 2025, "The human factor in cybersecurity: Addressing the risks of insider threats," *researchgate.net*, Accessed: Oct. 22, 2025. [Online]. Available: https://www.researchgate.net/profile/Hewa-Zangana/publication/386275073_The_Human_Factor_in_Cybersecurity_Addressing_the_Risks_of_Insider_Threats/links/674b1298f309a268c0193c7c/The-Human-Factor-in-Cybersecurity-Addressing-the-Risks-of-Insider-Threats.pdf

[13] A. Appari and M. E. Johnson, "Information security and privacy in healthcare: current state of research," *International journal of Internet and enterprise management*, vol. 6, no. 4, pp. 279–314, 2010.

[14] M. Boujettif and Y. Wang, "Constructivist approach to information security awareness in the Middle East," in *Broadband, Wireless Computing, Communication and Applications (BWCCA), 2010 International Conference on*, 2010, pp. 192–199.

[15] A. Mahfuth, "A Systematic Literature Review : Information Security Culture," pp. 1–6, 2017.

[16] A. Mahfuth, "Security Knowledge Required To Improve Employee Security Behavior in Information Security Culture," *International Journal of Computer Science and Information Security*, vol. 20, no. 2, 2022.

[17] R. MOHAMAD RASHID, O. ZAKARIA, and M. NABIL ZULHEMAY, "THE RELATIONSHIP OF INFORMATION SECURITY KNOWLEDGE (ISK) AND HUMAN FACTORS: CHALLENGES AND SOLUTION.," *J. Theor. Appl. Inf. Technol.*, vol. 57, no. 1, 2013.

[18] T. Ramluckan, B. van N. I. Martins, and others, "A change management perspective to implementing a cyber security culture," in *ECCWS 2020 20th European Conference on Cyber Warfare and Security*, 2020, p. 442.

[19] A. AlHogail and A. Mirza, "A proposal of an organizational information security culture framework," *Proceedings of International Conference on Information, Communication Technology and System (ICTS) 2014*, no. JANUARY 2015, pp. 243–250, 2014, doi: 10.1109/ICTS.2014.7010591.

[20] O. Huss, "Information Security Culture Guidelines: Based on Best Practices," 2025, Accessed: Oct. 22, 2025. [Online]. Available: https://www.diva-portal.org/smash/record.jsf?pid=diva2:1965097

[21] D. S. Hermawan, F. Setiadi, and D. Oktaria, "Measurement Level of Information Security Awareness for Employees Using KAB Model with Study Case at XYZ Agency," in *2022 1st International Conference on Software Engineering and Information Technology (ICoSEIT)*, 2022, pp. 174–179.

[22] M. Neri, F. Niccolini, and L. Martino, "Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment," *emerald.com*, vol. 32, no. 1, pp. 38–52, Jan. 2024, doi: 10.1108/ICS-05-2023-0084/FULL/HTML.

[23] A. Alhogail and A. Mirza, "Information Security Culture: A Definition and a Literature review," *Computer Applications and Information Systems (WCCCAIS)*, no. January, pp. 1–7, 2014, doi: 10.1109/WCCAIS.2014.6916579.

[24] A. Alhogail, "Design and validation of information security culture framework," *Comput. Human Behav.*, vol. 49, pp. 567–575, 2015, doi: 10.1016/j.chb.2015.03.054.

[25] J. Onyango, J. Onyango Abingo, D. Musumba, and D. Maina Mbuki, "Factors Influencing Information Security Culture in Organizations Dealing With Economic Crime in Kenya," *Abingo, IJSRM*, vol. 12, 2024, doi: 10.18535/ijsrm/v12i12.em12.

[26] A. Al Hogail, "Cultivating and Assessing an Organizational Information Security Culture; an Empirical Study," *International Journal of Security and Its Applications*, vol. 9, no. 7, pp. 163–178, 2015.

[27] J. F. Van Niekerk, "Establishing an information security culture in organizations: an outcomes based education approach," Nelson Mandela Metropolitan University, 2005.

[28] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, 2006.

[29] Bilal Khan, "Effectiveness of information security awareness methods based on psychological theories," *African Journal of Business Management*, vol. 5, no. 26, pp. 10862–10868, 2011, doi: 10.5897/ajbm11.067.

[30] J. Kaur and N. Mustafa, "Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME," *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, vol. 2013, pp. 286–290, 2013, doi: 10.1109/ICRIIS.2013.6716723.

[31] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Comput. Secur.*, vol. 42, pp. 165–176, 2014, doi: 10.1016/j.cose.2013.12.003.

[32] S. Mäeses, "Evaluation method for human aspects of information security," *Digi.Lib.Ttu.Ee*, pp. 1–56, 2015.

[33] J. Chmura, "Forming the Awareness of Employees in the Field of Information Security," *Journal of Positive Management*, vol. 8, no. 1, p. 78, 2017, doi: 10.12775/jpm.2017.006.

[34] A. Gandhi, "Quantitative assessment of information security awareness on informatics students in a university," *ACM International Conference Proceeding Series*, pp. 346–350, 2017, doi: 10.1145/3176653.3176728.

[35] M. S. bin Othman Mustafa, M. Nomani Kabir, F. Ernawan, and W. Jing, "An Enhanced Model for Increasing Awareness of Vocational Students Against Phishing Attacks," *2019 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)*, no. June, pp. 10–14, 2019, doi: 10.1109/i2cacis.2019.8825070.

[36] B. Aybars, S. E. -, D. ve T. B. D. Medical, and undefined 2025, "Human Factor Risk Modeling in Cybersecurity: A Scoping Review of KAB Frameworks and Data-Driven Approaches," *euroasiajournal.orgB Aybars, S ERDEMEuroasia Matematik, Mühendislik, Doğa ve Tıp Bilimleri Dergisi, 2025•euroasiajournal.org*, vol. 12, no. 1, pp. 47–59, 2025, doi: 10.5281/zenodo.15812726.

[37] B. Alkhazi, M. Alshaikh, S. Alkhezi, H. L.-I. access, and undefined 2022, "Assessment of the impact of information security awareness training methods on knowledge, attitude, and behavior," *ieeexplore.ieee.orgB Alkhazi, M Alshaikh, S Alkhezi, H LabbaciIEEE access, 2022•ieeexplore.ieee.org*, Accessed: Jan. 27, 2026. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9991148/

[38] B. H. Nguyen and H. N. Q. Le, "Investigation on information security awareness based on KAB model: the moderating role of age and education level," *emerald.comBH Nguyen, HNQ LeInformation & Computer Security, 2024•emerald.com*, vol. 32, no. 5, pp. 598–612, Nov. 2024, doi: 10.1108/ICS-09-2023-0152/FULL/HTML.

[39] D. S. Hermawan, F. Setiadi, and D. Oktaria, "Measurement Level of Information Security Awareness for Employees Using KAB Model with Study Case at XYZ Agency," in *2022 1st International Conference on Software Engineering and Information Technology (ICoSEIT)*, 2022, pp. 174–179.

[40] X. Jiang *et al.*, "Oral health-related knowledge, attitudes and behaviors (KAB) of dental students: a systematic review and meta-analysis," *bmcmededuc.biomedcentral.com*, vol. 25, no. 1, Dec. 2025, doi: 10.1186/S12909-025-07445-8.

[41] K.-L. Thomson, R. Solms, and L. Louw, "Cultivating an organizational information security culture," *Computer Fraud & Security*, vol. 2006, no. 10, pp. 7–11, 2006, doi: http://dx.doi.org/10.1016/S1361-3723(06)70430-4.

[42] A. Mahfuth, "Security Knowledge Required To Improve Employee Security Behavior in Information Security Culture," *International Journal of Computer Science and Information Security*, vol. 20, no. 2, 2022.

[43] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," *Journal of Computer Information Systems*, vol. 00, no. 00, pp. 1–16, 2020, doi: 10.1080/08874417.2020.1712269.

[44] A. Da Veiga and N. Martins, "Improving the information security culture through monitoring and implementation actions illustrated through a case study," *Comput. Secur.*, vol. 49, pp. 162–176, 2015.

[45] R. Von Solms and B. Von Solms, "From policies to culture," *Comput. Secur.*, vol. 23, no. 4, pp. 275–279, 2004.

[46] B. Von Solms, "Information security--the fourth wave," *Comput. Secur.*, vol. 25, no. 3, pp. 165–168, 2006.

[47] A. Da Veiga and J. H. P. Eloff, "A framework and assessment instrument for information security culture," *Comput. Secur.*, vol. 29, no. 2, pp. 196–207, 2010, doi: 10.1016/j.cose.2009.09.002.

[48] P. a. Chia, S. B. Maynard, and a. B. Ruighaver, "Understanding Organizational Security Culture," *Pacis*, pp. 1–23, 2002.

[49] M. E. Whiteman and H. J. Matort, *Principles of Information Security*. Cengage Learning, 2014.

[50] J. W. Brady, "Securing health care: Assessing factors that affect HIPAA security compliance in academic medical centers," in *System Sciences (HICSS), 2011 44th Hawaii International Conference on*, 2011, pp. 1–10.

[51] M. Siponen, S. Pahnila, and A. Mahmood, "Employees' adherence to information security policies: an empirical study," in *IFIP International Information Security Conference*, 2007, pp. 133–144.

[52] B. McIntosh, "An ethnographic investigation of the assimilation of new organizational members into an information security culture," Nova Southeastern University, 2011.

[53] A. Al Hogail, "Cultivating and Assessing an Organizational Information Security Culture; an Empirical Study," *International Journal of Security and Its Applications*, vol. 9, no. 7, pp. 163–178, 2015, doi: 10.14257/ijsia.2015.9.7.15.

[54] M. Alnatheer and K. Nelson, "Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context," *Australian Information Security Management Conference*, no. December, pp. 6–17, 2009.

[55] L. Connolly and M. Lang, "Information Systems Security: The Role of Cultural Aspects in Organizational Settings," *Information Systems Security*, 2013.

[56] M. A. Alnatheer, "A conceptual model to understand information security culture," *International Journal of Social Science and Humanity*, vol. 4, no. 2, p. 104, 2014.

[57] S. Dojkovski, S. Lichtenstein, and M. J. Warren, "Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia.," in *ECIS*, 2007, pp. 1560–1571.

[58] P. Ifinedo, "The effects of national culture on the assessment of information security threats and controls in financial services industry," *International Journal of Electronic Business Management*, vol. 12, no. 2, p. 75, 2014.

[59] E. Sherif, S. Furnell, and N. Clarke, "An identification of variables influencing the establishment of information security culture," in *International Conference on Human Aspects of Information Security, Privacy, and Trust*, 2015, pp. 436–448.

[60] J. F. Van Niekerk and R. Von Solms, "Information security culture: A management perspective," *Comput. Secur.*, vol. 29, no. 4, pp. 476–486, 2010, doi: 10.1016/j.cose.2009.10.005.

[61] J. H. P. Eloff and M. M. Eloff, "Information security architecture," *Computer Fraud & Security*, vol. 2005, no. 11, pp. 10–16, 2005.

[62] A. Da Veiga, N. Martins, and J. H. P. Eloff, "Information security culture – validation of an assessment instrument," *South African Business Review*, vol. 11, no. 1, pp. 147–166, 2007.

[63] C. Paulsen and T. Coulson, "Beyond Awareness: Using Business Intelligence to Create a Culture of Information Security.," *Communications of the IIMA*, vol. 11, no. 3, 2011.

[64] G. Dhillon and J. Backhouse, "Technical opinion: Information system security management in the new millennium," *Commun. ACM*, vol. 43, no. 7, pp. 125–128, 2000, doi: 10.1145/341852.341877.

[65] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, and T. Herawan, "Information security conscious care behaviour formation in organizations," *Comput. Secur.*, vol. 53, 2015, doi: 10.1016/j.cose.2015.05.012.

[66] A. Da Veiga and J. H. P. Eloff, "A framework and assessment instrument for information security culture," *Comput. Secur.*, vol. 29, no. 2, pp. 196–207, 2009.

[67] OECD, "OECD; 2005," in *The promotion of a culture of security for information systems and networks in OECD countries (OECD)*, 2005.

[68] C. Vroom and R. Von Solms, "Towards information security behavioural compliance," *Comput. Secur.*, vol. 23, no. 3, pp. 191–198, 2004.

[69] K. M. Parsons, E. Young, M. A. Butavicius, A. McCormac, M. R. Pattinson, and C. Jerram, "The influence of organizational information security culture on information security decision making," *J. Cogn. Eng. Decis. Mak.*, vol. 9, no. 2, pp. 117–129, 2015, doi: 10.1177/1555343415575152.

[70] S. M. Furnell, N. Clarke, R. von Solms, H. Kruger, L. Drevin, and T. Steyn, "A vocabulary test to assess information security awareness," *Information Management & Computer Security*, vol. 18, no. 5, pp. 316–327, 2010.

[71] A. Da Veiga and A. Da Veiga, "Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study," *Information & Computer Security*, vol. 24, no. 2, pp. 139–151, 2016.

[72] A. Nasir, R. A. Arshah, M. R. A. Hamid, and S. Fahmy, "An analysis on the dimensions of information security culture concept: A review," *Journal of Information Security and Applications*, vol. 44, pp. 12–22, 2019, doi: 10.1016/j.jisa.2018.11.003.

[73] A. Da Veiga, "Cultivating and Assessing Information Security Culture," *University ot Pretoria.*, 2008.

[74] R. M. Rashid, O. Zakaria, and N. Zulhemay, "Australian Journal of Basic and Applied Sciences Determining critical success factors (CSF) of information security knowledge (ISK) towards organisations ' information security effectiveness," vol. 8, no. 23, pp. 336–344, 2014.

[75] M. Whitman and H. Mattord, *Management of information security*. Nelson Education, 2013.

[76] M. Al-Awadi and K. Renaud, "Success factors in information security implementation in organizations," in *IADIS International Conference e-Society*, 2007.

[77] A. McIlwraith, *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*. Taylor and Francis, 2021. doi: 10.4324/9780429281785/INFORMATION-SECURITY-EMPLOYEE-BEHAVIOUR-ANGUS-MCILWRAITH.

[78] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," *Journal of Computer Information Systems*, vol. 00, no. 00, pp. 1–16, 2020, doi: 10.1080/08874417.2020.1712269.

[79] A. Alyami, D. Sammon, K. Neville, and C. Mahony, "Critical success factors for Security Education, Training and Awareness (SETA) programme effectiveness: an empirical comparison of practitioner perspectives," *emerald.com*, vol. 32, no. 1, pp. 53–73, Jan. 2024, doi: 10.1108/ICS-08-2022-0133/FULL/HTML.

[80] B. J. Oates, *Researching information systems and computing*. Sage, 2006.

[81] A. Pinsonneault and K. Kraemer, "Survey research methodology in management information systems: an assessment," *Journal of management information systems*, vol. 10, no. 2, pp. 75–105, 1993.

[82] O. Zakaria, "Investigating information security culture in a public sector organisation : challenges Malaysian a case," no. June, pp. 1–200, 2007.

[83] A. Bryman and E. Bell, *Business research methods*. Oxford University Press, USA, 2015.

[84] A. Al Hogail, "Cultivating and Assessing an Organizational Information Security Culture; an Empirical Study," *International Journal of Security and Its Applications*, vol. 9, no. 7, pp. 163–178, 2015, doi: 10.14257/ijsia.2015.9.7.15.

[85] O. Zakaria, "Understanding Challenges of Information Security Culture: A Methodological Issue.," in *In the 2nd Australian Information Security Management Conference, Securing the Future.*, Perth, Australia, 2004, pp. 83–93.

[86] J. F. Van Niekerk and R. Von Solms, "Information security culture: A management perspective," *Comput. Secur.*, vol. 29, no. 4, pp. 476–486, 2010, doi: 10.1016/j.cose.2009.10.005.

[87] N. Sohrabi Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," *Comput. Secur.*, vol. 56, pp. 1–13, 2016, doi: 10.1016/j.cose.2015.10.006.

[88] H. A. Kruger and W. D. Kearney, "Consensus ranking--An ICT security awareness case study," *Comput. Secur.*, vol. 27, no. 7, pp. 254–259, 2008.

[89] S. Al-umaran, "Culture Dimensions of Information Systems Security in Saudi Arabia National Health Services: A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy," no. February, pp. 167–171, 2015, [Online]. Available: https://www.dora.dmu.ac.uk/bitstream/handle/2086/11393/Thesis-1-June 2015-Final-v2.pdf?sequence=1&isAllowed=y

[90] M. Pattinson, K. Parsons, M. Butavicius, A. McCormac, and D. Calic, "Assessing information security attitudes: a comparison of two studies," *Information and Computer Security*, vol. 24, no. 2, pp. 228–240, 2016, doi: 10.1108/ICS-01-2016-0009.

[91] H. Liang and Y. Xue, "Understanding security behaviors in personal computer usage: A threat avoidance perspective," *J. Assoc. Inf. Syst.*, vol. 11, no. 7, p. 394, 2010.

[92] M. Leonard, S. Graham, and D. Bonacum, "The human factor: the critical importance of effective teamwork and communication in providing safe care," *Qual. Saf. Health Care*, vol. 13, no. suppl 1, pp. i85--i90, 2004.

[93] J. Hepler, "A good thing isn't always a good thing: Dispositional attitudes predict non-normative judgments," *Pers. Individ. Dif.*, vol. 75, pp. 59–63, 2015.

[94] N. S. Safa and R. Von Solms, "An information security knowledge sharing model in organizations," *Comput. Human Behav.*, vol. 57, pp. 442–451, 2016, doi: 10.1016/j.chb.2015.12.037.

[95] A. Mahfuth, S. Yussof, A. A. Bakar, B. Ali, and W. Abdallah, "A Conceptual Model for Exploring the Factors Influencing Information Security Culture," vol. 11, no. 5, 2017.

[96] M. Wilson and J. Hash, "Building an information technology security awareness and training program," *NIST Special publication*, vol. 800, p. 50, 2003.

[97] R. A. Amr, A. M. Al-Smadi, and R. T. Akasheh, "Diabetes knowledge and behaviour: a cross-sectional study of Jordanian adults," *Springer*, vol. 68, no. 2, pp. 320–330, Feb. 2025, doi: 10.1007/S00125-024-06304-3.

[98] A. Alhogail and A. Mirza, "Information Security Culture: A Definition and a Literature review," *Computer Applications and Information Systems (WCCCAIS)*, no. January, pp. 1–7, 2014, doi: 10.1109/WCCAIS.2014.6916579.

[99] I. Veseli, "Measuring the Effectiveness of Information Security Awareness Program," *Information Security*, 2011.

[100] G. A. Churchill, "Title Basic Marketing Research.," *The Dryden Press*, no. Fort Worth, 2001.

[101] J. F. Hair, W. C. Black, B. J. Babin, R. E. Anderson, R. L. Tatham, and others, *Multivariate data analysis*, vol. 5, no. 3. Prentice hall Upper Saddle River, NJ, 2006.

[102] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," *Journal of marketing research*, pp. 39–50, 1981.

[103] R. B. Kline, *Principles and practice of structural equation modeling*. Guilford publications, 2005.

[104] J. F. Hair Jr, G. T. M. Hult, C. Ringle, and M. Sarstedt, *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage Publications, 2016.

[105] J. E. Mathieu and S. R. Taylor, "Clarifying conditions and decision points for mediational type inferences in organizational behavior," *J. Organ. Behav.*, vol. 27, no. 8, pp. 1031–1056, 2006.

[106] M. S. Garver and J. T. Mentzer, "Logistics research methods: employing structural equation modeling to test for construct validity," *Journal of business logistics*, vol. 20, no. 1, p. 33, 1999.

[107] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, 2006.

[108] V. Marvik and R. Bakir, "Information security culture: An investigation into the impact of a large-scale cyberattack," University of Agder, 2023.

[109] T. Kizildeniz, F. B.-K. F. B. Dergisi, and undefined 2024, "Evaluating climate change knowledge, attitudes, and behaviors (kab) in agricultural sciences and technologies education," *dergipark.org.tr*, vol. 14, no. 2, pp. 619–633, 2024, doi: 10.31466/kfbd.1400642.

[110] I. Topa and M. Karyda, "Identifying Factors that Influence Employees' Security Behavior for Enhancing ISP Compliance," in *International Conference on Trust and Privacy in Digital Business*, 2015, pp. 169–179.

[111] R. MOHAMAD RASHID, O. ZAKARIA, and M. NABIL ZULHEMAY, "THE RELATIONSHIP OF INFORMATION SECURITY KNOWLEDGE (ISK) AND HUMAN FACTORS: CHALLENGES AND SOLUTION.," *J. Theor. Appl. Inf. Technol.*, vol. 57, no. 1, 2013.

[112] B. Von Solms, "Information security--the fourth wave," *Comput. Secur.*, vol. 25, no. 3, pp. 165–168, 2006.

[113] P. Singh, Y. F. Chan, and G. K. Sidhu, *A comprehensive guide to writing a research proposal*. Venton, 2006.

[114] J. Kaur and N. Mustafa, "Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME," *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, vol. 2013, pp. 286–290, 2013, doi: 10.1109/ICRIIS.2013.6716723.

[115] M. S. bin Othman Mustafa, M. N. Kabir, F. Ernawan, and W. Jing, "An enhanced model for increasing awareness of vocational students against phishing attacks," in *2019 IEEE international conference on automatic control and intelligent systems (I2CACIS)*, 2019, pp. 10–14.

[116] M. S. bin Othman Mustafa, M. Nomani Kabir, F. Ernawan, and W. Jing, "An Enhanced Model for Increasing Awareness of Vocational Students Against Phishing Attacks," *2019 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)*, no. June, pp. 10–14, 2019, doi: 10.1109/i2cacis.2019.8825070.

[117] A. Almoawi and R. Mahmood, "Applying the OTE model in determining the e-commerce adoption on SMEs in Saudi Arabia," *Asian Journal of Business and Management Sciences*, vol. 1, no. 7, pp. 12–24, 2011.

[118] O. Barzak, N. N. A. Molok, S. Talib, and M. Mahmud, "Information security behavior among employees from the Islamic perspective," *Proceedings - 6th International Conference on Information and Communication Technology for the Muslim World, ICT4M 2016*, pp. 211–215, 2017, doi: 10.1109/ICT4M.2016.46.

APPENDIX A.

ENGLISH QUESTIONNAIRE

Dear participant,

First of all, I would like to thank you for your valuable participation in this research survey, which aims to investigate of the security knowledge required for improving employee security behaviour in organisations as a part of a PhD research in Information Security Management.

Information security culture means that employees have the required values, beliefs and knowledge and behave accordingly in a way that protect the information assets (electronically or not) and to preserve the confidentiality, integrity, reliability and availability of information. For instance, updating antivirus, clear desk policy, strong password, regularly changing the password, not disclose private customer information and so on.

This study is directed at any persons working in the organisation. We assure you that your participation in the survey will be strictly confidential to the research team. Your personal details will be used for research classification purposes only and your identity will be kept anonymous and the name of the organisation will not be disclosed.

Your participation will contribute to obtain accurate results, and to improve the quality of research in information security in Palestinian organisations. Completing the questionnaire may take about 10 minutes. Please try to answer all statements. Each statement can be answered with only a single selection.

Should you have any further queries, please do not hesitate to contact us.

Again, we thank you for your interest and participation in this study.

Yours sincerely,

Amjad Mahfuth

PhD Student,

College of Computer Science & Information Technology
Tenaga National University, Malaysia
amahfouth99@gmail.com

Section A: Personal Information

The following section seeks are general information about you and your organisation. Please answer by ticking (√) in the appropriate bracket below:

Age :

☐ Under 25 ☐ 25 - 35 ☐ 36 - 45 ☐ Above 45

Year of experience:

How long have you been working in this organisation?

☐ Less than two year ☐ 2 - 4 Years ☐ 5 - 10 Years ☐ More than

Job Level:

What job level is applied to you?

☐ Hospital Management ☐ Doctor ☐ Nurse ☐ Administartive Staff

Education level:

☐ Undergraduate ☐ Postgraduate

Gender:

☐ Male ☐ Female

Working in IT department) :

Are you working in any area related to IT? e.g. IT department

☐ Yes ☐ No

Education Background in IT:

Was your education in IT related Field?

☐ Yes ☐ No

Work Requirements

Does your work require dealing with any computer or IT technology?

☐ Yes ☐ No

Security Awareness Training:

Have you got any security awareness training?

☐ Yes ☐ No

Section B: Security Knowledge's Construct's :

Please indicate your agreement to the following statements regarding the security knowledge construct's [1: Strongly Disagree; 2: Disagree; 3: Neutral; 4: Agree; 5: Strongly Agree]:

Knowledge of Security Threat		Please tick one				
		1	2	3	4	5
1.	I know the types of harmful threats to information assets.					
2.	I know the negative consequences of an attack on or threat to information assets.					
3.	I understand that security threats (attacks) can occur any time.					

4.	I know the threats and vulnerabilities towards the information assets in my work environment.					
5.	I know about information security threats.					
Knowledge of Organisation Information Security Strategy(information security policy, security requirements, standards and process)						
6.	I know what my organisation's information security strategy is.					
7.	I know my organisation's information security strategy helps me protect my organisation's information assets in my daily work.					
8.	I understand the content of information security strategy elements like policy.					
9.	I know organisation's information security strategy helps me understand what is expected from me as an employee in terms of safeguarding my organisation's information assets.					
10.	I know that my organisation has developed information security strategies to address the prevention and detection of threats and to respond to them.					
11.	Employees know information security requirements to protect information.					
12.	I am aware of information security policies related to my job such as the password policy.					
13.	I know that the information security is necessary to protect information in my organisation					
14.	I know that the information security is necessary to increase the confidence that the third parties have in my organisation.					
15.	I know information security practices such as data encryption.					
16.	I know information security practices such as a clear desk policy.					
17.	I know about information security controls (e.g. that I must set up a strong password).					
18.	I know the information security requirements helps me protect the information assets of my organisation.					
Knowledge of Security Technology						
19.	I know the technical tools and controls for information security helps me to preserve information security.					

20.	I know the security technology enables me to help other employees with their technical queries and problems					
21.	I know that the appropriate use of technical controls is vital to achieve information security.					
22.	I know the policy and guidelines for the effective use of information security hardware and software helps me preserve information security and prevent security breaches and threats.					
23.	I know how to use technical measures such as antivirus to ensure information security.					
Knowledge of legislation, regulations, national culture such as act Data Protection Acts, HIPPA, International Standards etc.						
24.	I know the government regulations regarding information security.					
25.	I am aware of relevant government information security related legislation such as copyrights.					
26.	I know the data protection and other relevant legislation and regulations.					
27.	I know the privacy and other relevant legislation and regulations.					
28.	I have clear directives on protecting sensitive and confidential information and applying the related regulations.					
29.	I am aware of the importance of the values of intellectual property and copy right laws.					
30.	I know the process of information security should not conflict with the society ethics and essential value.					
31.	I know the national culture must be taken into account when designing information security policy and guidelines.					
32.	I know the information security measures must comply with international standards.					
Knowledge of Security Responsibility						
33.	I know that information security is my responsibility in the organisation.					
34.	I know that I am responsible for any actions that conflict with information security requirements.					
35.	I know what information security is.					
36.	I know how to report information security incidents.					
37.	I know my role with regards to each security policy.					

38.	I know what to do when I detect a security violation.					
39.	I know what information assets to protect and how I can protect them.					
40.	I know that it is essential to protect information assets to achieve business success.					
41.	I am aware that I should never give my password to somebody else.					
Knowledge of Security Risk						
42.	I know that a weak password represents a security risk.					
43.	I know the risks when opening web links.					
44.	I know the security risks and dangerous to the information assets in my work environment.					
45.	I know the risk when opening e-mails from unknown senders, especially if there is an attachment.					
46.	I know the risk is when sharing passwords between others.					
47.	I know the risk is when giving out confidential information of visit prohibited internet sites.					
48.	I know it is essential to take care when talking about confidential information in public places.					

Section C: Security Behaviour:

Please indicate your agreement to the following statements regarding the security behaviour [1: Strongly Disagree; 2: Disagree; 3: Neutral; 4: Agree; 5: Strongly Agree]:

Security Behaviour		**Please tick one**				
		1	**2**	**3**	**4**	**5**
49.	I update the anti-virus software regularly.					
50.	I always lock my computer when I leave the desk.					
51.	I ensure that there is no confidential documents left on my desk when I leave the office.					
52.	When I suspect any information threat, I report it straightaway.					
53.	I should act in a way that prevents any threats to information security.					
54.	I share information about threats and vulnerabilities as appropriate.					
55.	I adhere to information security requirements in my organisation.					

56.	I act in a supportive manner to prevent, detect and respond to security incidents.					
57.	I behave carefully when I connecting with email attachments especially from unknown senders					
58.	I can easily ask question and leave comment regarded information security.					
59.	I usually follow my organisations information security strategy in my daily work to protect information assets.					
60.	I have a strong password.					
61.	I do not open email attachments if the content of the email looks suspicious.					
62.	Before reading an email, I will first check if the subject and the sender make sense.					
63.	I never give my personal information (like home/email address, telephone number, etc.) to unknown websites.					

Section D: Attitudes:

Please indicate your agreement to the following statements regarding the attitudes towards security knowledge's [1:Strongly Disagree; 2:Disagree; 3:Neutral; 4:Agree; 5:Strongly Agree]:

Attitudes (Attitudes towards Security knowledge)		**Please tick one**				
		1	**2**	**3**	**4**	**5**
64.	Knowing the types of security knowledge required in my organisation is necessary.					
65.	Knowing the types of security knowledge required in my organisation is beneficial.					
66.	My Attitude towards understanding the types of security knowledge required will have a positive effect on mitigating the risk of security breaches.					
67.	Knowing the types of security knowledge required in my organisation is a valuable.					
68.	My Attitude towards understanding the types of security knowledge required will have a positive effect on safeguarding the organisation's information assets.					
69.	My Attitude towards understanding the types of security knowledge required will have a positive effect on decreasing the risk of information security incidents.					
70.	My Attitude towards understanding the types of security knowledge required will have a positive effect on my security behaviour in my organisations.					

Thank You for Your Co-operation