ADOPTING THEORIES-BASED MODEL OF INFORMATION SECURITY COMPLIANCE BEHAVIOUR FOR HEALTHCARE EMPLOYEES IN KINGDOM OF SAUDI ARABIA

ALANAZI SULTAN TUWAYRISH S

UNIVERSITI SAINS MALAYSIA

2023

ADOPTING THEORIES-BASED MODEL OF INFORMATION SECURITY COMPLIANCE BEHAVIOUR FOR HEALTHCARE EMPLOYEES IN KINGDOM OF SAUDI ARABIA

by

ALANAZI SULTAN TUWAYRISH S

Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosophy

January 2023

ACKNOWLEDGEMENT

All praise and thanks are due to ALL MIGHTY ALLAH, for giving me the strength, health knowledge and patience to complete my Ph.D As the Prophet MOHAMMED "Peace be Upon Him" said: whoever does not thank people (for their favours) has not thanked Allah (properly), therefore, I would like to express my sincere gratitude and the deepest thanks to my supervisor Dr. Mohammed Anbar (main supervisor), DR. Shankar Karuppayah (co-supervisor), and DR. Shouki Abdullah Ahmed Ebad (field supervisor).

I will always be deeply in depth for their guidance, help, stimulating suggestions and encouragement which helped me in the research and writing of this thesis.

Most importantly, none of this could have happened without my family. “My Father” and my brothers, I really do not have any word to explain how much thankful I am for your assistance to make me who I am now, without you I am literally nothing. My mother who encouraged me and prayed for me throughout the time of my studies. And lastly, thanks to my lovely sisters. I love you all. Last but not least to my wife and children for their unlimited supported.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF ABBREVIATIONS

BDT	Behavioural Decision Theory
BI	Behavioural Intention
CMD	Cognitive Moral Development
CMDT	Cognitive Moral Development Theory
DOI	Diffusion of Innovation
GDT	General Deterrence Theory
H	Hypothesis
HBM	Health Belief Model
HISs	Healthcare Information Systems
IS	Information System
ISC	Information Security Culture
ISCB	Information Security Compliance Behaviour
ISCBMSDT	Information Security Compliant Behaviour Conceptual Model Based on The Self-Determination Theory
ISPC	Information Security Policy Compliance
ISPS	Information Security Policies
ISSP	Information System Security Policy
IT	Information Technology
KSA	Kingdom of Saudi Arabia
MCIT	Ministry of Communications and Information Technology
MOPTT	Ministry of Posts, Telegraphs and Telephones
NDMO	National Data Management Office
NS	Not Significant
PBC	Perceived Behavioural Control
PLS-SEM	Partial Least Square
PMT	Protection Motivation Theory
RCT	Rational Choice Theory
RH	Research Hypothesis
RO	Research Objective
RQ	Research Question
SD	Standard Deviation
SDAIA	Saudi Data and Artificial Intelligence Authority

SDT	Self-Determination Theory
SEM	Structure Equational Modelling
SETA	Security, Education, Training and Awareness
TAM	Technology Acceptance Model
TPB	Theory of Planned Behavior
TRA	Theory of Reasoned Action
UMP	Upper Management Practice

LIST OF APPENDICES

MENERIMA PAKAI TEORI BERASASKAN MODEL TINGKAHLAKU PEMATUHAN KESELAMATAN MAKLUMAT BAGI KAKITANGAN PENJAGAAN KESIHATAN DI KERAJAAN ARAB SAUDI

ABSTRAK

Penyelidikan keselamatan maklumat mendapati pekerja adalah punca masalah keselamatan dalam organisasi. Ia biasanya berlaku akibat mengabaikan dasar keselamatan maklumat (ISP). Oleh itu, isunya ialah bagaimana untuk meningkatkan tingkah laku keselamatan maklumat pekerja supaya ia mematuhi ISP. Kajian ini bertujuan untuk memajukan pengetahuan tentang tingkah laku keselamatan maklumat dalam industri penjagaan kesihatan Saudi, dengan fokus kepada kaedah untuk mempertingkatkannya dari sudut pandangan pekerja. Sorotan kajian menunjukkan penyelidikan tingkah laku pematuhan keselamatan maklumat (ISCB) masih tertumpu terutamanya pada set separa peramal, manakala kepercayaan agama, sifat keperibadian, dan undang-undang/hukuman tidak begitu mendapat perhatian. Inilah yang mencetus kajian ini dijalankan, iaitu untuk mencadangkan suatu model konsep tingkah laku pematuhan keselamatan maklumat berdasarkan model teori integratif. Dua fasa dalam penyelidikan ini ialah: (i) formulasi model hipotesis, dan (ii) pengenalpastian peramal ISCB. Berdasarkan model ini, soal selidik tinjauan (n = 433) telah dijalankan di Bandar Arar, ibu kota Wilayah Sempadan Utara di Arab Saudi dan maklum balas telah diterima secara rawak daripada pekerja hospital dan institut dengan kadar respons sebanyak 62.1%. Analisis statistik data berikut telah dijalankan: analisis faktor penerokaan, analisis kebolehpercayaan, analisis varians (ANOVA), regresi linear berganda, analisis korelasi pangkat Mann-Whitney, Kruskal Wallis dan Spearman. Oleh kerana nilai P lebih besar daripada 0.05, dapatan ujian Mann-Whitney

menunjukkan bahawa tidak terdapat perbezaan yang signifikan antara kumpulan jantina (p=0.148) atau status perkahwinan (p=0.169) dari segi ISCB. Selain itu, ujian Kruskal-Wallis menunjukkan tiada perbezaan kedudukan min yang signifikan secara statistik dalam tahap pendidikan berdasarkan kelayakan (p = 0.340, p >.05), pengalaman kerja (p = 0.251, p >.05), tempat kerja (p = 0.493, p >.05), dan kepakaran (p = 0.472, p >.05) berkenaan ISCB. Usia dan ICSB nampaknya tidak mempunyai perkaitan yang signifikan secara statistik, menurut keputusan analisis korelasi pangkat Spearman (r= -.009, n=5433, p = 0.846). Keputusan regresi linear berganda menunjukkan hubungan yang signifikan secara statistik antara kepercayaan agama (β = 0.217), efikasi kendiri (β = 0.223), undang-undang/hukuman (β = 0.147), ciri personaliti (β =0.166), norma subjektif (β = 0.152), dan keselamatan maklumat umum (β = 250) dan ISCB. Ini menunjukkan bahawa ICSB akan berubah masing-masing sebanyak 21.7%, 22.3%, 0.14.7%, 16.6%, 15.2%, dan 25%, jika kepercayaan agama, efikasi diri, undang-undang/hukuman, ciri keperibadian, norma subjektif, dan keselamatan maklumat umum meningkat sebanyak satu unit. Tambahan pula, keputusan R2 mendedahkan bahawa pembolehubah ini menyumbang 59.5% daripada variasi dalam ISCB, menjadikan model ini sesuai. Keputusan regresi linear berganda juga membayangkan bahawa kesan penyederhanaan kesedaran teknologi (β = 0.129) dan dasar keselamatan maklumat mungkin mempunyai kesan yang lebih besar ke atas ISCB pekerja penjaga kesihatan berbanding setiap pembolehubah secara berasingan. Selain itu, terdapat persamaan dan perbezaan antara pematuhan dari segi teori dan pematuhan sebenar bagi individu yang bekerja dalam bidang penjagaan kesihatan untuk peramal ISCB.

ADOPTING THEORIES-BASED MODEL OF INFORMATION SECURITY COMPLIANCE BEHAVIOUR FOR HEALTHCARE EMPLOYEES IN KINGDOM OF SAUDI ARABIA

ABSTRACT

Information security research shows that employees are a source of certain security difficulties in the organization. This frequently happens as a result of disregarding information security policies (ISPs). Therefore, the issue is how to enhance employee information security behaviour so that it complies with the ISPs. This study seeks to advance knowledge about information security compliance behaviour (ISCB) in the Saudi healthcare industry, with a focus on how it may be enhanced from an employee standpoint. A review of the literature suggested that research in information security behaviour is still predominantly focus on a partial set of predictors, while the religious beliefs, personality traits, and legal/punishment has not received as much attention. This resulted in the study being carried out to propose a proposed an information security compliant behaviour conceptual model based on integrative theories-based model. Two phases involved in this research were: (i) the hypothetical model formulation, and (ii) the identification of ISCB predictors. Based on this model, a survey questionnaire (n = 433) was carried out at in Arar city, the capital of the Northern Borders Province in the Saudi Arabia and responses were received randomly from the employees in hospitals and institutes giving a response rate of 62.1%. The following statistical analysis of the data was carried out: exploratory factor analysis, reliability analysis, analysis of variance (ANOVA), multiple linear regression, Mann-Whitney, Kruskal Wallis, and Spearman rank correlation analysis. Since the P-value was greater than 0.05, the Mann-Whitney test

findings revealed that there was no significant difference between gender groups (p=0.148) or marital statuses (p=0.169) in terms of ISCB. Additionally, the Kruskal-Wallis test revealed no statistically significant mean rank differences in educational levels based on qualifications (p = 0.340, p >.05), job experience (p = 0.251, p >.05), workplaces (p = 0.493, p >.05), and specialities (p = 0.472, p >.05) regarding ISCB. Age and ICSB appear to have no statistically significant associations, according to the results of the Spearman rank correlation analysis (r= -.009, n=5433, p = 0.846). The results of multiple linear regression showed a statistically significant relationship between religious beliefs (β = 0.217), self-efficacy (β = 0.223), legal/punishment (β = 0.147), personality traits (β =0.166), subjective norms (β = 0.152), and general information security (β = 250) and ISCB. This suggests that the ICSB will change by 21.7%, 22.3%, 0.14.7%, 16.6%, 15.2%, and 25%, respectively, if the religious beliefs, self-efficacy, legal/punishment, personality traits, subjective norms, and general information security increase by one unit. Furthermore, the R2 results revealed that these variables account for 59.5% of the variation in the ISCB, making the model a good fit. The results of the multiple linear regression also imply that the moderating effects of technological awareness (β = 0.129) and information security policy may have a greater impact on the on-healthcare employees' ISCB than they would have on each variable alone. Also, there were similarities and contrasts between the theoretical and actual compliance of individuals working in healthcare settings for ISCB predictors.

CHAPTER 1

INTRODUCTION

1.1 Introduction

This study investigates information security-compliant behaviour (ISCB) amongst employees in Saudi healthcare organizations. Through the conceptualization of a model, factors will be identified for the assessment of ISCB. The model will be conceptualized using the integrative theories-based model as the theoretical lens or perspective. Not only will the outcome(s) (i.e., the model) of this study provide an understanding of the factors influencing information security compliant behaviour, but the model will also assist the practitioner to develop methods for promoting ISCB.

Numerous organizations have admitted that technical solutions fall short of reducing security threats. This is because managerial elements also appear to be a security threat. Information security policy (ISP) compliance has emerged as a pressing concern for organizations as a result of managerial concerns (Kör & Metin, 2021; Siponen et al., 2007). Only if all employees adhere to the required ISPs can organizations effectively provide security education and support. ISCB describes an employee's behavior within a formal organization and their adherence to organizational information security rules, procedures, and standards (Connolly Lang, Gathegi, & Tygar, 2016). By taking these steps, the confidentiality of information, integrity, and quality of the information are all protected, and the employee's and the organization's reputations are upheld (DeLeon, 2021; Dong et al., 2021).

This chapter discusses the background of this study, information security compliance behavior as well as the motivation, problem statement, research questions, and objectives for this research study. The contributions and scope of the research are also discussed. Lastly, the chapter outlines the structure of the thesis.

1.2 Background

Information plays a significant role in the running of organizations. Information Systems (ISs) support organizations to achieve strategic competitive advantage over other organizations, such as assisting senior management in decision-making (Mai et al., 2017). They also help organizations in the timely implementation of projects and effective risk management (Wager et al., 2009). The use of information systems can result in many benefits for the healthcare providers, such as improving the quality of care, reducing medical errors, and enhancing the readability, availability, and accessibility of patients' information (Bowman, 2013; Lingamallu & Nayakvadi, 2018). A reliable and coherent information system requires a solid security framework that ensures the confidentiality, integrity, availability, and authenticity of critical information assets. Security is essential for organizations doing business in a globally networked and competitive environment while seeking to achieve their objectives and goals and ensuring business continuity (Faheem et al., 2017).

Recent reports indicate that the main threats to organizations' information systems, by more than 14%, are attributed to security incidents (Verizon, 2016). Employee behavior represents a significant variable in information security maintenance and information policy compliance. Employees can exhibit risky behavior which often threatens the security of information and information systems (Ifinedo, 2018; Mayer et al., 2017). Hwang et al. (2019) stated that insider threats are the consequences of misused actions, such as authority abuse, ignorance of policy, technical problems of software and hardware, and mishandling of information. It is not easy to control employees' behavior, which is considered the primary source of information security violations (Dinev & Hu, 2007). Most security breaches reported by

organizations have been attributed to employee behavior (Alshare et al., 2018), which creates significant security threats (Agyekum et al., 2019).

For these reasons, organizations usually establish their information system policies to enhance employees' awareness. Employees' awareness is the cornerstone of security compliance behaviour, prioritizing the differences and effects of awareness on security compliance behavior. Therefore, researchers have categorized the awareness types based on their role and relationship, such as technology awareness, information security awareness, threat awareness, etc. (Hwang et al., 2019).

Organizations around the globe today are highly dependent on the digital world where information systems and information security become the backbone of their daily operations. Organizations deploy security technologies and security management technologies to reduce risks to the security of their information and information systems (Faizi & Rahman, 2020; Hwang & Cha, 2018). Health organizations must identify methods that will assist them in securing electronic health records, to ensure the trust relationship between the patient and health care providers (Evans, 2016). Furthermore, most organizations develop and communicate information security policies aimed to guide their employees on doing and not in the digital world.

Unfortunately, research demonstrates that when proper information security behavior of employees is not taken into account, employees do not adhere to information security policies and these security technologies are vulnerable to human error and do not ensure the safety of information and information technology resources (Bhaharin et al., 2019). Hence, employee behavior plays a crucial role in the information security of all organizations, which means focusing on ISCB becomes vital (Kuppusamy et al., 2020).

There have been very few studies (such as Khan & Lutfi, 2021; Shaqrah & Noor, 2020; Zarour et al., 2021) conducted in KSA for predicting the variables influencing employees' ISCB in healthcare settings; this is either because of employees' unfamiliarity with patients' information privacy laws (Atiq & Alsulaiman, 2016), human psychological behavior, or non-compliance to the organization's security policy (Alsulaiman & Alrodhan, 2014). Therefore, there is a need to uncover and address the technical and non-technical reasons behind the violations of patients' confidential information in government hospitals in Saudi Arabia.

Furthermore, other variables that may influence the ISCB, such as employees' character, social, and psychology, including religious beliefs, personality traits, and punishments, also need to be studied because Saudi Arabia's culture is different from other cultures due to its strict religious and cultural commitments, especially on privacy (Alassafi, 2021). Although the information system in KSA has shown developments recently, not all hospitals have adopted good-featured systems of information security. This is because the delayed of conversion of systems from the medical record to health management systems. Moreover, the information system in some hospitals doesn't have enough well-trained and experienced administrators. The confidentiality and privacy of patient data and information must be ensured because the health care sector in Saudi Arabia is flawed with several security risks that may corrupt the integrity of patient data (Almaghrabi & Bugis, 2022). The health care system is facing many cybercrimes whereby hackers can gain access to confidential data and patient information (Almaghrabi & Bugis, 2022). There are several differences observed in the Saudi information security system when compared with the developed countries, especially the lack of good defensive systems like firewalls, encryption, intrusion prevention, network tunnelling, and packet filtering (Mishah *et al*, 2019).

One of the main challenges in the health sector is to protect the privacy of patients' data from leakage and tampering (Yang et al., 2020). Therefore, there is a need for a mechanism or a model, based on well-established theories to reduce the risk of data leakage or tampering by health sector employees or practitioners, including nurses and doctors (Hawthorne & Richards, 2017). There are several information systems already in use by some hospitals, but the element of confidentiality is lacking. Therefore, the researchers kept emphasizing the importance of information security systems to protect patients' privacy (Calero-Valdez & Ziefle, 2019).

For the time being, social engineering is considered one of the most inventive ways that have been used to gain illegitimate access to information systems and obtain sensitive or private information (Alsulami et al., 2021). It utilizes psychological manipulation to trick users into making security mistakes or giving away sensitive information. Besides, social engineering's success relies on the level of personnel compliance behavior, training, and competencies in securing sensitive information within their organizations (Algarni, 2019). Therefore, organizations require to assure that their personnel recognizes as much as possible about information security and the impacts of these threats and attacks.

Likewise, the other countries, the Kingdom of Saudi Arabia is vulnerable to social engineering, and as reported by Kaspersky, the KSA recorded approximately 1,000,000 social engineering attacks (*i.e.*, phishing attacks) in the quarter of 2020 (AlMindeel & Martins, 2020). Consequently, it is vital for organizations, especially the financial and medical sectors due to their sensitivity and criticality, to improve their users' awareness of social engineering attacks to mitigate their impact and occurrences.

In addition, the average total cost of a data breach in Saudi Arabia and the UAE combined is $5.31 million, a 7.1 percent increase since 2017, according to tech giant

IBM Security (Truly news, 2022). The results of a Middle East study examining the full financial impact of a data breach on businesses located in the two Gulf countries found that breaches cost companies $163 per lost or stolen record on average. It also revealed that the root cause for 61 percent of breaches in Saudi Arabia and the UAE is malicious or criminal attacks, followed by system glitches at 21 percent and human error at 18 percent (Truly news, 2022). According to Altamimi et al.(2019), additional research should be conducted to identify additional awareness strategies and training opportunities (face-to-face interactions, online courses, and seminars) that are operational health care measures to stop these employees from rationalizing their improper behaviour.

All these issues are considered the motivation for the present research to highlight the importance of these variables. It is also the first research to investigate the effects of predictors, including religious beliefs, punishment, and personality traits, on the ISCB of healthcare workers in the Kingdom of Saudi Arabia's hospitals.

1.2.1 Information Security Compliance Behavior

As defined by Griffin and Neal (2000), ISCB is "a set of core Information System activities that need to be carried out by individuals to maintain information security". Besides, Chan *et al*. (2005) defined ISCB as" a set of skills needed to perform the required actions and is also influenced by a conducive information security climate

ISCB of employees is considered a vital concern in IS protection, especially in cases of carelessness, inattentiveness, or intentional action such as clicking on links in phishing emails, disclosing confidential information to family and friends, or searching for personally identifiable information on their families (Li & Hoffman, 2018). Another challenge addressed by Hu *et al*. (2012) was information security management by highlighting the differences among variables of data protection, such as organization,

individual, and technical variables that influenced the organization's information security (Hu *et al*., 2012). Researchers believed that insider threats are more severe and dangerous than outsider threats because employees typically have inside knowledge of the organization's security policy and methods to access the information system (Bulgurcu et al., 2010; Siponen & Vance, 2010). The security violation statistics point to the difficulty in identifying information theft incidents by employees. For example, 59% of ex-employees admitted attempting to steal confidential information (Symantec, 2009); 44% of the respondents reported abusing their computers (Richardson, 2008); and 50% of Information Technology (IT) managers carried full responsibility of insider threats to employees of the organization (Li & Hoffman, 2018).

1.2.2 Information Security in Saudi Healthcare System

To define the legal framework for the use of computers or information networks, as well as the violations of the requirements, Saudi Arabia created an anti-cybercrime law in March 2007 (Alshammari & Singh, 2018). This law specifies such crimes and establishes their penalties to ensure information security improvement and the protection of rights relating to the appropriate use of computers and information networks. Preservation of the public interest, morals, and shared values, as well as the protection of the national economy, are characteristics of an anti-cybercrime law (Alshammari & Singh, 2018). For instance, any person who commits unauthorized access to cancel, delete, destroy, leaking, damage, alter, or redistribute private data shall be subject to imprisonment for a period not exceeding three years and a fine not exceeding 3,000,000 riyals, or either penalty (https://laws.boe.gov.sa).

Information security and privacy in the healthcare sector is an issue of growing importance (Al-Janabi *et al*., 2017). The adoption of digital patient records, increased regulation, provider consolidation, and the increasing need for information between

patients, providers, and payers, all point toward the need for better information security (Atkinson *et al*., 2018). With the beginning of the technological era and the fourth industrial revolution, all government sectors use technology services after realizing the importance and advantages of digital systems compared to the traditional paper-based system. Technology systems in KSA, including individual information systems, are deployed in all government institutions with a clear vision based on the foundation of its value goals (*i.e.*, be beneficial and benefit the community) (Abokhodair *et al*., 2017).

One of the current trends in Saudi Arabia is the interest in a holistic view of healthcare service together with the development work for its improvement to provide easy access to all health services to citizens and residents by bringing the essential technical systems that facilitate these services (Helal & Elimam, 2017). However, it is worth-mentioning that Saudi Arabia is a developing country and the transformation to a fully computer-based system in the healthcare sector started during the last decade, where the process of developing and advancing its technical services is still ongoing (Aljuaid et al., 2016).

The government has been generously supporting and promoting the healthcare sector to keep pace with the developed countries, medical and technical systems. Researchers are aware that healthcare providers own and maintain a massive amount of patients' data and private health information during their review of hospitals and healthcare institutions (Dash et al., 2019; Jamshed et al., 2015). This data is one of the main pillars of health organizations, if not the basis for them. Therefore, it may be subject to breach attempts, leaks, or disruption. Perhaps one of these methods can exploit the weak point, as a means to destroy or leak the data to achieve their vested interests.

1.2.3 Saudi Arabia Law for Data Protection

There are laws in Saudi Arabia to protect the privacy of patients' data (Hausawi, 2016) derived from the Quran and Sunnah but may not be applied or just a metaphor, but, there is no comprehensive law under the Saudi legal system that specifically provides for data protection excepting some provisions scattered here and there under some legislations. Besides, there is a lack of national laws to protect patients' electronic records, which may be due to the lack of awareness or expertise, or both, to formulate and enforce such laws (Elgujja & Arimoro, 2019). The KSA generates, gathers, and stores huge amounts of data that have essential potential to contribute to its economic development and the welfare of its citizens. To support the accomplishment of its data value, the KSA has developed the Data Management and Personal Data Protection Standards to govern and manage the practice of data and create an efficient data-driven institution across government parties (Brazeau & Wright., 2022). Additionally, to complete the comprehensive regulatory framework for data protection, the National Data Management Office adopted Data Management and Personal Data Protection Standards in January 2021 (White Label Consultancy, 2022).

However, the standards of data management and personal data protection include the controls and specifications across fifteen variables as listed in below Figure 1.1, which depicts the KSA framework for data management and personal data protection that stretch the data lifecycle from creation, storage, movement, usage, till retirement (SDAIA, 2021). Personal data is defined as every piece of information, regardless of its origin or format that may be used to individually identify a person or that could enable someone to do so indirectly. This includes name, personal identity number, addresses, phone numbers, license numbers, documents, personal property,

bank account, and credit card numbers, as well as other information of a personal nature (White Label Consultancy, 2022).

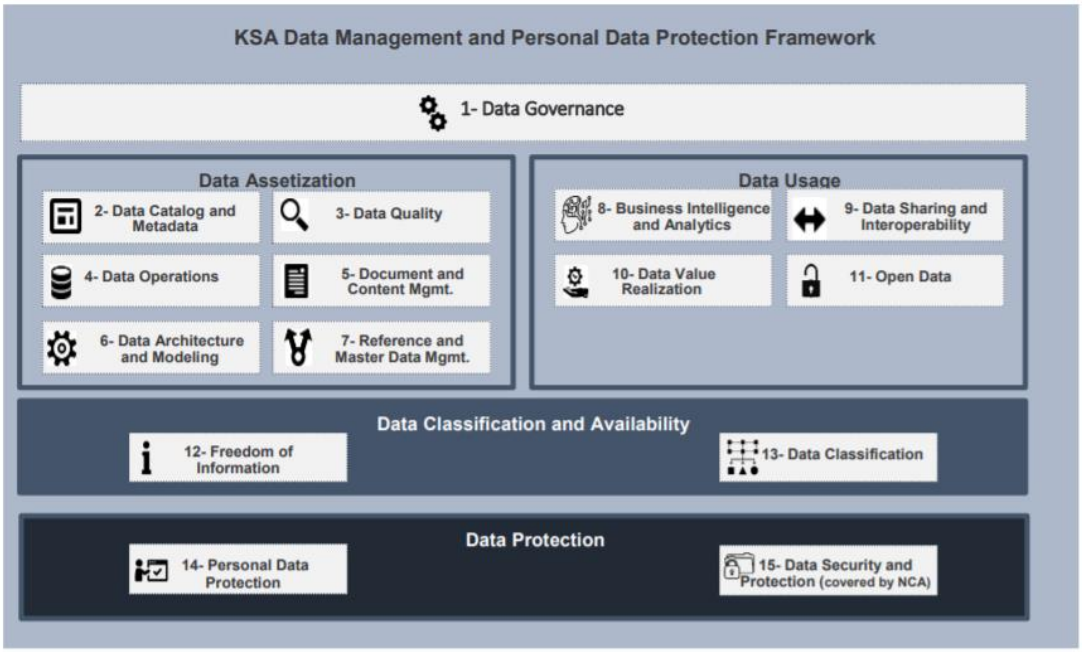

Figure 1.1 For Data Management and Personal Data Protection (SDAIA, 2021).

1. Data Governance: Data Governance grants planning and implementation of the organization's data management procedures power and control through individuals, organizations, and technologies.
2. Data Catalog and Metadata: Data Catalog and Metadata aim to make it easier to access integrated high-quality metadata.
3. Data Quality: Data Quality focuses on enhancing the organization's data quality and making sure that data is appropriate for its intended usage in light of consumer needs.
4. Data Operations: To maximize the value of data, this area focuses on designing, implementing, and supporting data storage.
5. Document and Content Management: The capture, storage, access, and usage of documents are all under the control of document and content management.

6. Data modelling and architecture: Data Architecture and Modelling focus on creating formal data structures and data flow channels to enable end-to-end data processing across and within entities.
7. Reference and Master Data Management: all crucial data can be linked to a single master file using reference and master data management, creating a single point of reference for all crucial data.
8. Analytics and Business Intelligence: Analytics and Business Intelligence focus on analyzing an organization's data records to get insight and make judgments regarding the data discovered.
9. Data sharing and interoperability: Data sharing and interoperability entails the gathering of data from multiple sources and comprises integration strategies that support a smooth exchange of information across various IT components on the inside as well as the outside.
10. Data Value Realization: Data Value Realization entails a continual analysis of data assets to identify possible revenue-generating or cost-saving data-driven use cases for the company.
11. Open Data: Open Data focuses on the organization's data that might be made accessible to the general public to improve transparency, spur innovation, and support economic growth.
12. Freedom of Information: The freedom of information field is concerned with giving Saudi citizens access to government data, outlining the procedure for doing so, and outlining the appeals process in the event of a dispute.
13. Data classification: Data classification entails classifying data to effectively use and safeguard it.

1.2.4 Healthcare Sector in the KSA

The healthcare sector in the KSA caters to a rapidly growing population, along with the simultaneous increase in health issues and the increased awareness that is causing the sector to thrive. The information security of health organizations has shown development recently in KSA, in terms of standards, procedures, and policies (SADAIA, 2021). The KSA is continuously investing in healthcare-related projects in several regions, including Riyadh, Makkah, Jeddah, etc. Many studies on information security in the healthcare sector have offered new strategies to safeguard healthcare-related data, especially when faced with cutting-edge cybercrimes. The following section looks into prevalent healthcare challenges in terms of ISCB in the KSA.

1.2.5 Healthcare Challenges in Term of ISCB in KSA

As the 5th common space after land, sea, air, and outer space; cyberspace requires legal measures, cooperation, and coordination (Schjolberg & Seminar, 2012). A new international legal mechanism is sought to protect against the escalation of cybercrimes (Schjolberg & Seminar, 2012).

The KSA has enacted a law against cybercrime. On March 26th, 2007, Royal Decree no. M/17 8 Rabi 1 1428 / 26 March 2007 had been decreed as the Anti-Cyber Crime Law. Its goal is to fight against cybercrimes by detecting the crimes and installing punishments to ascertain the following:

1. Improve data security,
2. Safeguard rights of the legitimate use of data networks and computers,
3. Safeguard common values, public interests, and morals, and
4. Safeguard the national economy.

AlQahtani (2016) claimed that as many Saudi Arabians end up in jail for being clueless about committing cybercrimes, it is imminent to inform the citizens of the KSA

about laws enacted against cybercrimes via mass media. A major motivation to initiate Information Technology (IT) in the Arab Gulf region is to support the new policy on managing foreign labor flow as a result of social and economic issues that stemmed from uncontrollable foreign labour flow (Al-Gahtani, 2003).

Rapid IT progress poses a challenge in the KSA. Upon realizing the significance of establishing digitalized government information, the KSA issued a Royal Decree no. A/2 in May 2003, which changed the name of 'The Ministry of Posts, Telegraphs, and Telephones (MoPTT)' to 'Ministry of Communications and Information Technology (MCIT)'. As stipulated in the Saudi Arabia Royal Decree (7/B/2427) dated 16/1/1424H, its finance ministry had established an e-government program. In 2005, both the finance ministry and MCIT established YESSER – an e-government programme.

The implementation of HIS offers numerous advantages to healthcare organizations, including better access to information, enhanced service quality, and lower medical glitches. Although the KSA supports the deployment of HIS in mimicking developed countries, it has several barriers within its HIS, *i.e.*, technological hurdles and poor information security awareness.

Despite the increasing demand for e-commerce (Al-Gahtani, 2003), organizations must weigh in on user acceptance of IT transformation to ensure successful IT adoption. In many cases, end-users are expected to accept IT usage just because the organizations have done so. Additionally, the slow progress of IT across developing countries has been attributed to political instability, poor infrastructure, social factors, exorbitant costs, and language barriers (Al-Gahtani, 2003).

To execute total or partial information security systems in the KSA, many organizations tend to hire outsourcing companies, primarily to develop and maintain hardware, software, and integrated ISs; to train the staff; and to educate end-users

(Alkahtani, 2018). Saudi firms hire more than one supplier to avoid mission abortion due to outsourcing risk. Apart from enhancing organizational IT competence, outsourcing improves the efficiency and quality of information services with IT professionals.

Meanwhile, some setbacks of outsourcing information security systems in Saudi firms are unqualified individuals dealing with security issues, low service provider credibility, mishandling of intellectual property and company secrets, as well as a potential breach of data security (Alkahtani, 2018). As a developing country, the KSA is still in its infancy stage for applying networking computers. The protection of IS has been recognized by the Saudi MCIT (MCIT website, 2011), but almost all partial or total deployment of information security systems is handled by outsourcing companies.

1.3 Research Motivation

Several major factors are driving this research. First, the use of information technology has become widespread in the healthcare industry, which, like other businesses, involves a variety of stakeholders, including the patient, the healthcare practitioner, researchers, and third-party payers. As a result, there are security risks presented by the use of an automated health information system (HIS), such as unauthorized access or failure to meet information security goals, as well as unauthorized use of health information applications and resources. The personal health information contained in the patient record, in whatever form it takes, must be adequately safeguarded. Healthcare practitioners, as users, pose the greatest risk because their ignorance or blunders may compromise this data. They understand the significance of security compliance but do not put it into practise. Logins and passwords were found to be widely shared among healthcare practitioners.

Health-care workers offer a serious information-security risk. When compared to other industries, there is less security awareness and little information security management. ISCB is among these solutions. With the understanding of employee ISCB, the results of this study will reveal what might help healthcare organizations effectively reduce policy violations by employees. The importance of user security behavior in the research of ISCB is becoming more widely recognized. This study aims to develop aggressive and dynamic ISCB among healthcare employees within the context of their work. The goal is to employ the proposed integrative theories-based model as a motivational tool to promote ISCB.

The Islamic religion is a part of Saudi culture and plays an important role in the lives of Saudis. Saudi Arabian culture is distinct from other cultures due to the religion of Islam, the role of history, and its heritage. As a result, religious beliefs may have an impact on the security of information systems, and the creation of this information security framework is of great relevance to all. Individuals frequently fail to comply with Information Security Standards, which require health care members to adhere to security procedures. Unfortunately, violations and noncompliance by employees with Information Security Standards continue to be major challenges for Saudi enterprises. Specifically, a lack of religious values may place some duties beyond the employee's capacity and increase the likelihood of human mistake. While earlier research has revealed a variety of factors that influence such compliance, few have focused on religious views. Understanding Saudi Arabian cultural distinctions, such as religious beliefs, can have a significant impact on a health care organization's success and security. As a result, this research seeks to know how religious beliefs could enhance ISCB in the Saudi environment.

1.4 Problem Statement

Healthcare employees' awareness of information security regulations and commitment to security policies is rather low in Saudi Arabia (Basfar & Bajunaied, 2020). Since most information security incidents rise in the number of hackers targeting patient data in the Saudi health system result from the failure by employees to comply with ISPs (Almaghrabi & Bugis, 2022), Saudi hospitals need to ensure that employees follow policies and regulations to mitigate information security risks and avoid potential risks that may breach patient confidentiality. Therefore, developing data security rules are crucial to limit the risk of jeopardizing patient data integrity and safety. The Anti-Cyber Crime Law was enacted by Royal Decree No. M/17 on 8 Rabi 1 1428 / 26 March 2007 to prevent cybercrime by identifying and punishing such offenses to ensure 1increasing data security 2) protection of legitimate computer and information network use rights, 3) protecting the public interest, morals, and shared values, and 4) protecting the national economy (Alkahtani, 2018). However, the majority of Saudi online users are not yet completely utilizing this low, and some users are unaware of it to a considerable extent (Alkahtani, 2018).

Furthermore, health organizations have faced significant security breaches not only because of technological mistakes but also because of inadequate security culture, security awareness, and security management among the organizations' workers, according to Almaghrabi and Bugis (2022). The implementation of an effective information security policy compliance framework among Saudi health organizations has not yet been fully implemented due to the absence of flaws in security and policy systems, a lack of employee awareness, and unfavorable environmental conditions (; Alfawaz et al., 2010; Alnuem et al., 2011; Mishah et al., 2019; Shaban, 2015). Although the framework for data management and personal data security (Figure 1) can be used

by any knowledge-intensive organization in Saudi Arabia to ensure and enforce employee compliance, low human compliance may also hinder the successful implementation of a healthcare information security system. In their analysis of electronic security in Saudi hospitals, Mishah et al. (2019) discovered that the health information management departments lacked adequate training. The authors also discovered that only 33.33% of hospitals maintained updated antivirus software, 83.3% of hospitals lacked electronic security officers, and only 33.33% of hospitals had firewall security, which is a serious shortcoming.

Furthermore, the framework for data management and personal data protection does not include information on the security of the user's computer or the frequency of infractions of the online access restrictions (Figure 1). One flaw is that this formwork does not contain any instances of violating online access rules of any kind. The Personal Data Protection Law, which went into effect in September 2021 and required organizations to make numerous adjustments to their regular daily operations to ensure their compliance with this novel legislation, is the only reference for applicable data protection laws in the Saudi Arabia region (Almaghrabi & Bugis, 2022). However, this won't be put into effect until March 2023. Due to this regulation, data controller information must be registered, processing records must be kept, improved governance over such personal data must be enforced, and data subject rights (Saudi Arabia’s data protection law, 2022).

In contrast, the majority of prior studies—including those by Alkahtani (2018), Ryutov et al. (2017), and Box & Pottas (2013)—ignored critical elements that impacted the ISCB, including legal/punishment, personality traits, and religious beliefs. In other words, most of the prior studies, both local and international, did not cover these factors (*i.e.,* legal/punishment, personality traits, and religious beliefs) affecting ISCB.

Similarly, the impact of religious beliefs, personality traits, and legal punishment on employees' ISCB in KSA has not yet been studied. Therefore, the ISCB in Saudi Arabia and the impact of these factors are still questionable to a large extent (AlHariri & Al-Hattami, 2017). There is a need for evaluating the religious beliefs of the ISCB in Saudi Arabia since Islam is the main religion and most of the citizens follow the instructions derived from the Quran and Sunnah. In addition, the culture of Saudi Arabia has religious commitments to the information of others. Therefore, religious beliefs are considered the main variable that should be preserved for getting successful IS. Part of the research focus for this particular thesis is on cybercrime and its association with legal punishment in Saudi Arabia. To date majority of the victims of cybercrimes in the country still fail to report their cybercrime experiences to law enforcement agencies. This is to some extent because of the common belief that cybercrime is not an offense that is punishable in Saudi Arabia or as a result of the lack of awareness of the existence of the laws related to cybercrimes within the country. This may also be due to the belief that Saudi Arabia does not have a robust legal system concerning cybercrimes (Alabdulatif, 2018).

In addition, Saudi people have personality traits that differ from other cultures (Tolah, Furnell & Papadaki, 2021; Al Garni & Cooke, 2021). Also, personality traits are an essential variable of security models against cybercrimes in Saudi Arabia (Qashqari et al., 2020). Employees' unique personality traits, such as agreeableness, conscientiousness, extraversion, neuroticism, and openness, have an impact on their intent to follow information security standards, with neuroticism frequently resulting in security policy infractions. To present a better understanding of human personality traits and identify organizational predictive values for security behaviour, Tolah, Furnell and Papadaki (2020) discovered that personality traits increase security awareness among

Saudi employees, increasing the degree of their organizational security cultures' support for security-compliant behavior. The findings showed that agreeableness, conscientiousness, and openness are three personality qualities that significantly influence employees' behavior and attitudes toward information security culture levels. This thesis seeks to make a difference in this respect by analyzing the impact of personality traits on ISCB in Saudi healthcare. Therefore, legal/punishment, personality traits, and religious beliefs play a significant role in a better attitude and behavior of the employee and might have a positive impact on the security concerns of information security.

Among the theories frequently employed in ISCB studies are the theories of planned behavior (TPB) (Ifinedo 2014), protection motivation theory (PMT) (Torten, Carmen, & Stephen, 2018), and general deterrence theory (GDT) (Johnston et al., 2016). Future supporting hypotheses will be built on the findings of PMT, TPB, and GDT, which were deemed to be the most pertinent. However, there is no synthesis of theory or creation of hybrid models that incorporate various ISCB facets (Sulaiman et al., 2022). Based on the application of the core theory, the modified theories might not have substantial empirical support. According to the TPB (Ajzen, 1985), there is still a disconnect between intention and conduct, which is mostly due to the approximately one-third of people who express a positive intention to exercise but do nothing about it. As a general theory of motivation, PMT was created to explain human behavior in terms of the dangers of those acts.

Apart from that, the majority of existing studies such as (Etim et al., 2021; Gangire et al., 2021; Hwang et al., 2019) have only adopted a single theory evaluation of the model, and thus it might cause loss/lack of generalization of the existing models. Even though, the studies used integrative models such as (Kim et al., 2014; Iriqat *et al.*,

2019), still suffered from the inconsistency of definition, use, and/or the level of self-efficacy measurement, and method of evaluating the relationship in the context of security behavior. However, these models were not commonly used to test the ICSB in the Saudi environment. Ifinedo (2012) proposes that the combination of PMT and TPB offers a better knowledge of the variables influencing an employee's compliance with cyber security. In terms of cyber security, TPB and PMT have been found to work well together to predict information security behavior (Safa et al., 2015). According to GDT, people will refrain from committing crimes if they face rapid, severe punishment and a degree of conviction (Alshare et al., 2018). In addition, the impact mechanisms of GDT have been evaluated in diverse and multi-cultural ways, but the ICSB primarily in Saudi Arabia has not been addressed. Due to the great difficulty in articulating the justification for these theories in studies of cyber and information security, very few research incorporate more than two theories (Sulaiman et al., 2022). This study integrates TPB, PMT, and GDT to examine the variables impacting ISCB in the context of Saudi healthcare, thereby filling the knowledge gap. The objective of this thesis is to study these theories and their effect on the ISCB, primarily in undergraduate employees at hospitals.

Therefore, there is an urgent need to propose an integrative model to be applied in healthcare institutions to find out the factors that impact information security and safeguarding all information resources from privacy and security violations. The statement of the problem of this research can be summarised as follows:

- Weakness in implementing the regulations of security of Saudi healthcare systems due to barriers and influencing factors.
- Most of the existing local studies neglected some of the predicators that affect the ISCB in KSA healthcare, and only focus on a partial set of predictors.

- Still, no clear association between cybercrimes with legal/punishment, personality traits, and religious beliefs in the Saudi healthcare sector.

1.5 Research Objectives

The main goal of this research is to propose an integrative theories-based model for ISCB in the Saudi healthcare sector to be adapted as a security policy or used as guidelines to improve ISCB among their employees and prevent data privacy leakage. The following objectives are set to achieve the primary goal of this research:

1) To identify a set of variables that might affect the ISCB in the Saudi healthcare sector.
2) To determine whether the legal/punishment, personality traits, and religious beliefs influence information security compliant behaviour of employees in the Saudi healthcare sector.
3) To assess the effectiveness of the proposed integrative theories-based model by comparing the association results with the results of the state-of-the-art models adopted in ISCB.

1.6 Research Questions

Based on the research problem statements stated in the previous section, the research study's objective described above, and the study's purpose, the following questions will be relevant:

1) What are the variables that might affect the ISCB Saudi healthcare sector?
2) What significant relationship exists amongst legal/punishment, personality traits, self-efficacy, religious beliefs, and information security compliant behaviour of employees in the Saudi healthcare sector?

3) How does the integrative theories-based model perform in evaluating the ISCB of healthcare professionals efficiently?

1.7 Research Contributions

The significance of this study is reflected through its potential contributions to the body of knowledge regarding ISCB specifically for the improvement of practice, theory, and methodology.

1.7.1 Theoretical Contributions

The theoretical significance lies in the aim of the study which is to propose a model for the ISCB among employees in the Saudi healthcare sector. This is significant as the proposed combined multi-theories in information security research, particularly information security behaviour. It is envisaged that this study will contribute to the expansion of an existing body of knowledge by developing a conceptual model based on an integrative theories-based model. Developing a conceptual model based on an integrative theories-based model, this research as it allows for a better explanation of the ISCB among employees in the healthcare industry, notably in the KSA. In this way, the integration theories-based model highlights the impact of factors like legal/punishment, personality traits, and religious beliefs on the ISCB of employees. By producing a model based on these factors, this study will close this gap and also improve our understanding of the information security behavior of employees in the healthcare sector in the KSA. Consequently, it may contribute more knowledge to the existing studies in the general area of ISCB in the field of health care, as recent academics emphasizing the need to examine compliance with information security policies.

In meeting the research objectives, this very study applies and integrates TPB, GDT, PMT, TAM, DOI, and other theories to explain o ISCB in the healthcare sector. As pre-factors of intent to comply, behavioral beliefs about compliance and knowledge of compliance factors such as self-efficacy, subjective norms, cost of compliance and non-compliance, general information security, and technology awareness with the ISCB are also discussed in this study. These factors were not taken into account in earlier research studies in an integrative theories-based model. This study examined how Saudi employees' adherence to information security policies was impacted by extended TPB, GDT, and DOI with PMT, behavioral, and technological aspects. Additionally, this study emphasized the part that information security behavior's antecedent elements played. To improve ISCB among employees, this study intends to evaluate ISCB in the Saudi healthcare sector. It may be used to develop security policies as guidance for health care organizations.

According to the literature, this study added to the body of knowledge by giving practical and pragmatic information on the ISCB in healthcare care. Although some studies are available on the concerned topic, most are in developed countries such as the USA, and some are qualitative. Most studies normally conceptualized the factors influencing the ISCB in healthcare but did not analyze the relationship or connection between the factors. This study conceptualized the factors influencing ISCB healthcare and did practical tests to provide information on legal/punishment, personality traits, religious beliefs, self-efficacy, subjective norms, cost of compliance and non-compliance, general information security, technology awareness, and employees' behavior of information security compliance.

By combining the rationale choice theory with the DOI Theory, this study addresses a gap in the literature on ISCB. Expanding specific focus on ISCB in the

healthcare of Saudi Arabia that is influenced by “cost of compliance and non-compliance, general information security, and technology awareness.” Furthermore, this research was noteworthy since it was based on a newly created model for ISCB in healthcare that combined multi-theories. The majority of behavioral models are based on well-known behavior theories such as TPB and PMT. CMDT and RCT are two theories of human behavior discussed in this study.

1.7.2 Methodological Contributions

This particular study uses a quantitative research methodology to achieve its goals, which includes using a questionnaire as a data-gathering tool. As a result, it is important because it offers a questionnaire that modifies relevant scales from several trustworthy sources to fit the conceptualization and operationalization of the factors that influence ISCB as they relate to the study's environment. By analyzing data using "Structural Equation Modeling (SEM)" methods to analyze relationships among factors to better understand ISCB among employees in the Saudi healthcare industry, this study greatly adds to the growth of cyber security studies and literature. The study employed Smart-PLS to test hypotheses and find potential connections between variables that showed to be crucial in fostering information security compliance behavior. After examining the measurement model, the study has shown that the used measurements are reliable and valid. Confirmatory factor analysis is used to further validate that the questionnaire items are related to the identified variables. As a result, it demonstrates that the metrics utilized are likewise relevant in Saudi Arabia.

This study utilizes regression analysis to determine the most significant variables influencing ISCB among employees in the Saudi healthcare industry. Multiple linear regression was also used to find the predictors of ISCB for participants of the present research. Furthermore, this study adds to the field's methodology by employing