



**Daffodil**  
*International*  
**University**

**Information security policy compliance model in organizations:**

**Social bond theory**

**Submitted By**

Tahsin Haider

ID: 191-35-422

Department of Software Engineering

Daffodil International University

**SupervisedBy**

Dr. Imran Mahmud

Associate Professor & Head

Department of Software Engineering

Daffodil International University

**Date of Submission: 15<sup>th</sup> December 2022**

## APPROVAL

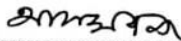
This thesis titled on “**Information security policy compliance model in organizations: Social Bond Theory**”, submitted by **Tahsin Haider (ID: 191-35-422)** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

### BOARD OF EXAMINERS



Chairman

-----  
**Dr. Imran Mahmud**  
**Head and Associate Professor**  
Department of Software Engineering  
Faculty of Science and Information Technology  
Daffodil International University



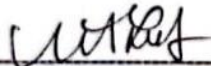
Internal Examiner 1

-----  
**Afsana Begum**  
**Assistant Professor**  
Department of Software Engineering  
Faculty of Science and Information Technology  
Daffodil International University



Internal Examiner 2

-----  
**Dr. Md. Fazle Elahe**  
**Assistant Professor**  
Department of Software Engineering  
Faculty of Science and Information Technology  
Daffodil International University



External Examiner

-----  
**Mohammad Abu Yousuf, PhD**  
**Professor**  
Institute of Information Technology  
Jahangirnagar University

## DECLARATION

I announce that I am writing this study document under Dr. Imran Mahmud, Associate Professor and Head, Department of Software Engineering, Daffodil International University. I therefore state that this work or any portion of it was not proposed here therefore for Bachelor's degree or any graduation.

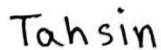
**Supervised by:**



---

Dr. Imran Mahmud  
Associate Professor and Head  
Department of Software Engineering  
Daffodil International University

**Submitted by:**



---

Tahsin Haider  
ID: 191-35-422  
Department of Software Engineering  
Daffodil International University

## ACKNOWLEDGEMENT

In today's world of competition there is a race for survival in which they have to come forward for success. First of all, I would like to thank the Almighty Allah Who has clearly guided me to do the right thing in life. Without His grace this topic could not have become a reality. And my parents, whom I am extremely indebted to for bringing me to this stage with love and encouragement.

I feel compelled to talk about the opportunity to study at Daffodil International University. I would like to sincerely thank Prof. Dr. Imran Mahmud, Head of the Department of Software Engineering. Full of all the respected teachers who enjoy teaching me an interesting and understandable way. I am grateful for having them on my journey.

I am obligated to guide Daffodil International University to guide them through the constant supervision of Dr. Imran Mahmud to provide the necessary information as well as to honor the initiative and additionally their help in completing the research. Finally, I would like to express my gratitude to my batch mates, members of DIU for their kind co-operation and consolation that has helped me to accomplish this task.

## ABSTRACT

The internet and other forms of information technology have had a huge impact on people's everyday lives. However, individuals and organizations still place a significant amount of importance on the protection of sensitive data. When it comes to information security, humans should be taken into consideration in addition to technological factors. Technology alone is not sufficient to provide a secure environment for information. Users might be irresponsible, obstinate pranksters, don't care enough about information security, don't care at all, or don't care enough to make errors because they don't know enough about information security. A novel model was developed for the purpose of this research, which reveals how the conduct of workers is impacted by how effectively they follow the information security regulations of their firm. The way in which attachment, commitment, and personal standards were conceived of is the most essential aspect of this study. All three of these concepts are crucial components of the Social Bond Theory. The analysis of the data revealed that there are a number of factors that have a significant impact on how employees feel about adhering to the organization's information security policies. These factors include the sharing of information security knowledge, working together, intervening, and having experience. On the other hand, workers' attitudes on adhering to the information security policy are not much impacted by attachment. The findings also indicate that an employee's attitude may be influenced by the degree to which they are committed to their job as well as by their own personal standards. The level of compliance with organizational rules concerning information security is significantly impacted not only by one's attitude but also by one's behavioral intention with respect to information security compliance.

**Keywords:** *Attitude structural equation, Information security, Confirmatory factor analysis, Information security awareness, Structural equation modelling, Involvement.*

## TABLE OF CONTENTS

1	Introduction.....	1
1.1	Background.....	1
1.2	Problem In Bangladesh.....	2
1.3	Problem Statement.....	2
1.4	Research Objective.....	3
1.5	Research Question.....	3
1.6	Organizations of the chapter.....	3
2	Literature review.....	5
3	Theoretical Background.....	6
3.1	Social bond theory.....	6
3.2	Theory of involvement.....	7
4	Conceptual framework and hypotheses.....	8
4.1	Information security knowledge sharing.....	8
4.2	Information security collaboration.....	9
4.3	Information security intervention.....	10
4.4	Information security experience.....	10
4.5	Attachment, commitment and personal norms.....	11
5	Methodology.....	14
5.1	Data collection.....	14
5.2	Demography.....	14
6	Data Analysis& Discussion.....	17
6.1	Measurement model.....	17
6.2	Construct Reliability.....	17
6.3	Discriminate Validity.....	18
6.4	F <sup>2</sup> .....	19
6.5	Structural model.....	19
6.6	Coefficient of determination (R <sup>2</sup> ).....	19
6.7	Research result.....	20
6.8	Discussion.....	20
7	Conclusion, limitations and future work.....	23
8	Questionnaire.....	24
9	References.....	26

# 1 INTRODUCTION

## 1.1 Background

Web-based technology have benefited companies and consumers, but data breaches remain a concern. Anti-virus, anti-malware, anti-spam, anti-phishing, anti-spyware, firewall, authentication, and intrusion detection systems are technical components of information security, but they cannot ensure data protection (Herawan, 2015). Hackers target people, not systems. Bad information security behaviors include using a social security number as a user name and password, writing passwords on sticky paper, discussing passwords with colleagues, reading emails from strangers and downloading attachments, and installing software from the Internet. Information security should include people and technology (Furnell and Clarke, 2012). To decrease information security breaches, you must deploy many security methods.

Hackers always find new methods to bypass security on the Internet (Safa et al., 2014). Fake disk defragmentation and anti-virus scanners are new approaches to fool consumers into believing their PC is infected. These programs often falsely report issues and recommend installing spyware-laden freeware (Kim et al., 2015). Organizations may mitigate these assaults by exchanging information.

Von Solms and Van Niekerk investigated many cyber security topics in 2013. Information security, which covers availability, integrity, and privacy, is different from cyber security, even though they have many similarities. Cybersecurity extends beyond information security. People and society are involved here. It may be damaged, unlike information security, which always causes indirect harm. Organizations must collaborate to secure information and cyberspace (Werlinger et al., 2009).

Information security breaches cost firms money and reputation (Safa and Ismail, 2013). Proper information security behavior reduces organizational information security breaches. Employee information security knowledge reduces company risk, according to research (Abawajy, 2014; Arachchilage and Love, 2014). (2014). Both residential and business users need information security knowledge, according to Kritzinger and von Solms (2010). This

research also found that distribution strategies and enforcement components matter. Experience in information security may raise awareness. Information security expertise improves understanding, familiarity, and incident management (Safa et al., 2015). (2015).

## **1.2 Problem In Bangladesh**

Reports indicate that the existing legislative framework in Bangladesh does not offer the conditions necessary to put a halt to the misuse of personal data. This allegation is substantiated by the countless examples of recorded breaches of privacy that occur every day in Bangladesh. The right to one's own privacy is recognized as a fundamental principle in Bangladeshi law. In addition, unethical activity undermines national integrity, contributes to the additional expenses of cybercrime, and cultivates a lack of confidence in internet service providers. For example, in 2016, hackers from North Korea were successful in transferring \$81 million from the central bank of Bangladesh. This was made possible because a Bangladesh Bank employee fell for a phishing link between the months of March and October of that year (Bangla tribune, 2021). In addition, the organization has had severe ramifications as a direct result of these activities, including a loss of financial resources, harm to its image, and allegations of abuses of personal privacy.

## **1.3 Problem Statement**

Studies also demonstrate that organizations that ignore individuals fail (Li et al., 2010; Stanton et al., 2005; Webb et al., 2014). Experts recommend protecting data from several angles (Herath and Rao, 2009). Companies invest in information security technologies and tools but often don't pay enough attention to their personnel; therefore security incidents and breaches still occur (Ifinedo, 2012). ISOPs are effective and efficient strategies to enhance staff information security practices (Crossler et al., 2013; Son, 2011).

However, research has revealed that workers don't follow information system security regulations, which safeguard a company from abuse, destruction, and exploitation (Vance et al., 2012). ISOP-compliant employee information security behavior is crucial for security (Woon and Kankanhalli, 2007). Ifinedo (2014) examined how social bonds affect employee information security compliance. The Social Bond Theory emphasizes attachment to the company, dedication to its policies and programs, engagement in specific activities like



information security, and the idea that information security behavior is necessary to protect informational assets.

Cheng et al. (2013) discussed how corporations violate information security regulations in another research. The research found that workers who feel more connected to their company are less inclined to transgress regulations and behave badly.

This study aims to make staff safeguard information in accordance with rules. Involvement, attachment, commitment, and personal standards from the Social Bond Theory will be examined (SBT). Understanding sharing, cooperation, intervention, and experience impact how workers work on information security problems and improve awareness and knowledge of information security, which is vital to this study.

#### **1.4 Research Objective**

**RO1:**The purpose of this research is to improve the information security behavior of employees in accordance with information security policies and procedures. The involvement, attachment, and commitment of employees, as well as the personal norms that derive from the Social Bond Theory, are the focus of this research (SBT).

**RO2:**The purpose of this study is to propose a conceptual framework that illustrates the process by which businesses achieve compliance with information security policy.

#### **1.5 Research Question**

**RQ1:** Does the research seek to increase and diversify research on information security organizational policy compliance?

**RQ2:** Does Information security knowledge sharing of SOCIAL BOND THEORY(SBT) play any role in mitigating the risk of information security breaches?

#### **1.6 Organizations of the chapter**

The subsequent parts of this article are organized in the following manner so as to provide a more in-depth examination of the thesis. The second chapter is a survey of the relevant literature, in which the research gaps and prior publications on information system security behavioral objectives are investigated. In Chapter 3, which follows Chapter 2, we had a

discussion about the theoretical backdrop. In Chapter 4, we were tasked with coming up with hypotheses and then discussing them. In Chapter 5, we discuss topics such as sample size and demographics, measurement items and data analysis methods. We also discuss research methodology, which includes data-collecting processes, demographic information, and data analysis methods. In Chapter 6, we discuss the findings that resulted from the data analysis. In Chapter 6, I went through the findings and discussed them. In Chapter 7, we went through the Conclusion, as well as some of the Limitations and Future Work.

## 2 LITERATURE REVIEW

ISOPs increase staff information security practices (Crossler et al, 2013; Son, 2011). However, research has revealed that workers don't follow information system security regulations, which safeguard a company from abuse, destruction, and exploitation (Vance et al, 2012). Cheng et al. (2013) and Ifinedo (2014) have discussed how workers who implement information security rules reduce the chance of breaches in firms. We employed the same social relationship elements as previous research. Information was collected using Likert scales and questionnaires. Each question is about a build item from prior investigations (Cheng et al, 2013; Ifinedo, 2014; Tamjidyamcholo et al, 2014; Witherspoon et al, 2013). Sharing information security knowledge increases awareness and understanding, which impacts ISOP compliance. This finding matches Rocha Flores et al. (2014) and Tamjidyamcholo (2015). (2014). Information security experience deepens and realigns workers' ISOP compliance views (Rhee et al, 2009). The attachment impact on ISOP compliance was not statistically significant, contradicting H5. Fortunately, the statistical study demonstrated a substantial correlation between commitment and ISOP support. Ifinedo observed similar results (2014). Finally, statistical testing demonstrated that ISOP followers' feelings strongly influence their goals. This supports previous research (Ifinedo, 2014; Siponen et al, 2014).

### **3 THEORETICAL BACKGROUND**

The Internet has offered individuals from all walks of life—regardless of their social, educational, political, or economic status—a new means to communicate that is distinct from the traditional methods. Cybersecurity breaches are still a major concern for professionals in this industry. The results of this study demonstrate that ensuring ISOP compliance is a viable strategy for lowering the probability of data breaches inside a business. We built a conceptual framework using concepts from the Social Bond and Participation Theories that demonstrates how workers' commitment, attachment, involvement, and personal norms might influence their attitude toward adhering to information security rules and procedures in enterprises.

In this research, taking part in the SBT has taken the position of information security knowledge exchange, cooperation, intervention, and experience. This action was taken in light of the nature and implications of SBT involvement. The Involvement Theory has taught us a lot about information security knowledge sharing, teamwork, intervention, and learning from mistakes. More information on the theories and factors, as well as how they operate, will be provided below.

#### **3.1 Social bond theory**

To determine how successfully workers were adhering to the ISOP, the SBT was employed. The SBT has gained attention from academics in recent years. In 1969, Hirschi proposed the SBT on the basis that males had an innate bias toward criminal behavior. One of the main points of the SBT is that a person's propensity to engage in criminal behavior decreases as their network of supportive relationships grows. This is a crucial aspect of the theory, and it's what compels us to use it in our quest to improve compliance with established norms for data protection. Bad behavior is more common when social bonds are frayed or disrupted. Attachment, Involvement, Commitment, and Individual Norms are the four fundamental concepts that form the basis of this paradigm. These are distinct components, yet they must be assembled as a whole. One's propensity to violate the norms of an organization decreases in proportion to the degree to which he or she identifies with that group (Chapple et al., 2005).

Historically, the SBT has also been used to the question of adolescent delinquency. A person's propensity to engage in antisocial conduct is influenced by his or her attachment to conventional significant people, dedication to conventional objectives, participation in conventional activities, and acceptance of the veracity of common value systems. In this scenario, they either partially or completely disregard what is required of them by law or by the duties they have taken upon themselves (Mesch, 2009; Veenstra et al., 2010). Over time, SBT's applicability expanded to include adult-level criminal behavior and internal organizational issues. The likelihood of insider computer misuse is significantly reduced, as shown by Lee et al. (2004), when people have a sense of connection, commitment, engagement, and beliefs about the system. Information security breaches may be mitigated when staff members act in accordance with established rules and processes, as discussed by Cheng et al. (2013) and Ifinedo (2014). We replicated these research and utilized the same measures of social connections. The primary components in this study model are loyalty to the organization, dedication to organizational policies and plans, participation in information security, and the conviction that adhering to organizational information security rules and procedures is necessary to secure information assets.

### **3.2 Theory of involvement**

How much time, energy, and attention someone invests in a task is the focus of the Involvement Theory (Lee et al., 2004). Customers, goods, students, and more have all benefited from the use of the Involvement Theory. According to Rocha Flores et al. (2014), a lack of staff engagement in information security is one possible explanation for a lack of knowledge and concern about security among employees. People's emotions are manifested in many ways depending on their level of involvement. Knowledge sharing, teamwork, taking the initiative, and experience are all indicators of how invested an employee is in the protection of the company's data. In other words, there are a variety of methods to get active, and they all entail sharing knowledge about information security, working together, becoming involved, and earning experience. The purpose of this research is to determine whether there is a correlation between employee knowledge, cooperation, assistance, and experience in the field of information security, and adherence to the rules and procedures established by the firm.

## **4 CONCEPTUAL FRAMEWORK AND HYPOTHESES**

In this investigation, we come up with a fresh model that demonstrates how ISOP guidelines are adhered to. The research model incorporates the concepts derived from both the Social Behavior Theory and the Involvement Theory. The structure may be broken down into two primary components. In the first section, we discuss the many methods in which individuals may get engaged in information security. These include the exchange of information security knowledge, the working together of individuals and groups, the intervention of individuals, and the gaining of experience. Attachment, commitment, and personal standards are the topics that will be covered in the second section of this discussion on SBT's fundamental components. In the paragraphs that follow, we'll go into more detail regarding each of these topics.

### **4.1 Information security knowledge sharing**

Acquired by study or experience, knowledge is an in-depth familiarity with a topic, fact, piece of information, value, or set of skills. It is much easier for a group to come up with a solution, generate new ideas, or implement new rules and procedures when everyone has access to the same information (Wang and Noe, 2010). Organizational knowledge is the sum of a company's data, information, and the expertise of its people when they are all shared effectively. These are priceless resources that aid in decision-making, boost productivity, lessen danger, and lower expenses (Lee et al., 2011).

A smart method to demonstrate you care about information security and increase awareness is to share information about it. Experts in this industry all deal with the same issues, thus they must be able to provide effective solutions. By pooling resources and knowledge, we may save time and money by avoiding the need to create duplicate solutions to the same issues (Feledi et al., 2013). The resources saved from not having to develop new security solutions might be used toward enhancing those that already exist. However, as was shown in a recent research, one of the biggest challenges in this area is convincing experts to share their expertise. Information security awareness may be greatly aided by the dissemination of relevant anecdotal experience (Rhee et al., 2009). In 2014, Tamjidyamcholo and Sapiyan Bin Baba investigated the impact of knowledge sharing on information security in online

communities. Members' reluctance to share their expertise was also cited as a major barrier to the exchange of information security-related data.

The task of cyber security is difficult, and users' understanding may greatly lower the likelihood of security mishaps (Ben-Asher and Gonzalez, 2015). According to Arachchilage and Love's (2014) study, individuals may prevent phishing simply by being aware of the threat. Clarity and ambiguity coexist in the realm of knowledge. It is evident that there is knowledge that may be recorded, categorized, summarized, and disseminated in the form of written papers, instructions, and even films. The folks who possess implicit knowledge have it stored in their own brains. Not much is known about it since it has not been documented (Rocha Flores et al., 2014). Knowledge sharing concerning information security does double duty: it raises awareness and demonstrates an organization's commitment to the topic. It has been said that one of the most influential factors in how individuals really feel about engaging in an activity is their level of awareness of it (Abawajy, 2014). We assumed the following based on the information provided above:

Information security practices are more likely to be adopted by staff when they are encouraged to disseminate their own knowledge of best practices.

**H1:** When employees share what they know about information security, it makes them more likely to follow ISOP.

## **4.2 Information security collaboration**

People collaborate to execute a job or achieve a goal. Collaboration involves participation, companionship, and occasionally teamwork. It's a cycle of individuals, teams, or organizations working together to achieve objectives. Information security specialists collaborate to gather, integrate, categorize, disseminate, and share their knowledge with other experts and workers. When information security issues arise, Ahmad et al. advised communicating and cooperating (2012). Technical teams and staff may communicate using the issue tracking system.

This cooperation helps retain records, organize work, and collect incident-handling proof. Collaboration involves providing knowledge, enhancing it, offering comments, and having peers evaluate it (Feledi et al., 2013). Collaboration helps uncover information security threat

assessment aspects (Mace et al., 2010). In 2007, Bernard investigated information lifecycle security risk assessment to solve these security flaws. Information security council members working collaboratively to address important information risk is recommended. IT security, audit, HR, legal, complaints, risk management, corporate security, and other departments are represented. Together, they disclose information security breaches, making this field smarter. Information security cooperation helps users understand security breaches. Working together saves information security firms money on knowledge capture and processing. We think:

**H2.** Collaboration on information security has a positive effect on how employees feel about following ISOP.

### **4.3 Information security intervention**

Participation, debate, and group reflection enhance information security awareness (Albrechtsen and Hovden, 2010). Seminars, lectures, online learning and conversations, sending messages and emails, blogging, videos, and newsletters may teach individuals about information security and demonstrate companies care. These technologies revolutionize how individuals and businesses see, comprehend, and forecast cyber security (Shaw et al., 2009).

Internet security is vulnerable due of its size. Hackers find private, accurate, or unavailable information in several ways. Cyberspace changes constantly, so users should stay informed (Stanton et al., 2005). Relevant, current, and continuous security awareness initiatives are most vital. Parsons et al. (2014) examined how users' behavior changes when they know and follow organizational regulations. Their study demonstrated that intervention improves organizational policy knowledge and that information security policy knowledge is connected to policy attitudes. Information security interventions raise awareness of Internet, email, social engineering, passwords, and reporting events.

**H3.** Information security interventions change the way employees feel about following ISOP.

### **4.4 Information security experience**

One gains knowledge, competence, and insight into a situation or topic via experience. Experts are recognized as leaders in their respective fields because of their extensive knowledge in them. According to the parameters of this research, "experience with information security" refers to both a familiarity with information security incidents and the



ability to avoid, manage, and lessen the risk associated with such occurrences. Knowledge and experience, risk analysis and management, information about incidents and weaknesses, strategy and planning, process and procedures, policies and standards, methodologies and frameworks, training, audits, contracts, and outsourcing are all different aspects of information security management, as outlined by Ashenden (2008). Intriguingly, this study found that both education and experience ranked highly. To better understand how users' past encounters affect information security, Albrechtsen (2007) investigated their impact. According to the findings, a lack of knowledge and expertise among users is the primary cause of information security issues. Acting appropriately in the actual and ever-evolving environment requires knowledge and experience (Internet). Consequently, let's assume:

**H4.** Employees are more likely to follow ISOP if they have experience with information security.

#### **4.5 Attachment, commitment and personal norms**

Attachment, commitment, engagement, and belief are the four primary criteria outlined by Hirschi (1969) that reveal how individuals interact with social structures. According to the SBT, a person who has stronger social relationships is less likely to engage in antisocial behavior. When social relationships are frayed or severed, criminal activity increases. When it comes to teenagers' social connections, dedication to their objectives, participation in extracurriculars, and shared moral convictions, this theory provides a compelling explanation for their risky behavior. All of these factors contribute to antisocial adolescent behavior including teen drinking and driving, cigarette and drug use, and other forms of rebellion (Chapple et al., 2005; Mesch, 2009).

In recent years, the Social Bond Theory has been used to explain why workers adhere to information security standards and procedures established by their employers (Cheng et al., 2013; Ifinedo, 2014). Social bond theory has been expanded to include organizational dysfunction. When workers feel more connected to their employers, they are less likely to engage in white-collar crime. When the connection between a corporation and its workers is strained or severed, employees are more likely to act in an antisocial manner. When people identify with a group, they are more inclined to behave according to its norms.

Attachment is the emotional connection that individuals feel to others they care about. Partners in the workplace may include other employees, managers, employers, or even larger

entities. Those who have close relationships with others are less prone to engage in harmful behaviors (Cheng et al., 2013). Workers are looking to their managers for assistance. Therefore, they value the admiration of such individuals. Their performance is evaluated by their superiors, who then determine whether or not to promote them. Employees perform better when they show loyalty to their managers and take their recommendations (Zhai et al., 2013). This motivates the following proposal:

**H5:** The attachment has a good effect on how employees feel about following ISOP.

When it comes to the human element of information security, people pose the greatest threat since they have direct contact with the data that has to be protected. Within this industry, their information security responsibilities and their desire to do so are of the utmost importance (AlHogail, 2015). The desire to get a job that has a high rank is an example of commitment. People who are devoted to something consider their own achievement and reputation to be vital (Cheng et al., 2013). They devote more time and effort to their work in order to achieve greater levels of achievement. People who are serious about their professional lives will not take the risk of breaching regulations that might endanger or even destroy their professions (Lee et al., 2004). Because of this, workers who care more about the firm are less likely to violate the security standards than their coworkers who care less about the organization. Consequently, the following concept is proposed:

**H6:** Commitment has a good effect on how employees feel about following ISOP.

Information security personal norms are the beliefs and practices of an organization's personnel that are consistent with the company's own rules. Lee et al. (2004) investigated how individual standards shape appropriate computer behavior. A survey of the literature reveals that individuals' propensity to violate established policies on information security inside an organization is influenced by cultural norms (Lee and Kozar, 2005; Ng et al., 2009). Individuals with high moral fiber are presumed to be more compliant with data security regulations enacted by their employers. This motivates the following proposal:

**H7:** Personal norms make employees more likely to follow ISOP because of how they feel about it.

One's attitude may either be positive or negative, depending on how they feel about the activity in question. A person's emotional investment in a subject might influence the way they see it (Hepler, 2015). What influences a person's outlook is their history and the present. A person's attitude reflects their feelings toward various entities. These might be either good or extremely bad. Whether or if an employee follows an organization's information security rules is influenced by how they feel about such regulations, according to the area of information security (Siponen et al., 2014). We believe that an upbeat outlook on the company's information security rules increases the likelihood that they will be followed. From this, we may draw the following conclusion:

**H8:** The way employees feel about following ISOP has a positive effect on their intentions to follow ISOP.

## 5 METHODOLOGY

### 5.1 Data collection

The data was collected from workers at different companies in Bangladesh that had implemented sound information security practices to safeguard their data.

Everyone involved utilized the Internet and a web-based system in their various roles. In order to get their thoughts on the questionnaire's wording, usefulness, and instrument understanding, we had them fill it out in front of a researcher after providing a short description of the study's goals. Our success depended on winning their acceptance. We assured them that the data would be used only in an academic capacity and would be kept in strictest secrecy at all times. After receiving their approval, we sent the questionnaire to them.

### 5.2 Demography

Both of these approaches were used to acquire the data. Both paper-based and online versions of the questionnaires were used in the process of data collection. Participants each received one of the 150 surveys that were sent their way after being sent using the sharing options of Google Forms. A total of 143 persons participated in the survey. On the other hand, we distributed fifty questionnaires (hard copy). Having a total of forty replies as a result. The demographic information of the participants is summarized in Table 1, which may be seen below. The participants' educational backgrounds and genders are broken down into further detail in Table 2, which may be seen below.

		<b>Your Gender</b>			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		43	19.9	19.9	19.9
	1.Male	82	38.0	38.0	57.9
	2.Female	91	42.1	42.1	100.0
	Total	216	100.0	100.0	

Table 1: Gender

		<b>AgeGroup</b>			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Teen	40	18.5	23.1	23.1
	Young	66	30.6	38.2	61.3
	Middle aged	39	18.1	22.5	83.8
	Matured	28	13.0	16.2	100.0
	Total	173	80.1	100.0	
Missing	System	43	19.9		
Total		216	100.0		

**Table 2: Age**

### Number of years of working experience

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	39	18.1	22.5	22.5
	2	15	6.9	8.7	31.2
	3	38	17.6	22.0	53.2
	4	28	13.0	16.2	69.4
	5	28	13.0	16.2	85.5
	12	11	5.1	6.4	91.9
	16	14	6.5	8.1	100.0
	Total	173	80.1	100.0	
Missing	System	43	19.9		
Total		216	100.0		

### Level of education

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		43	19.9	19.9	19.9
	3. Bachelor's degree	78	36.1	36.1	56.0
	4. Master's degree	56	25.9	25.9	81.9
	5. Ph.D. degree	39	18.1	18.1	100.0
	Total	216	100.0	100.0	

### Current Position

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		43	19.9	19.9	19.9
	1.Top management personnel	82	38.0	38.0	57.9
	2.Mid-level personnel	66	30.6	30.6	88.4
	3.Junior Staff	25	11.6	11.6	100.0
	Total	216	100.0	100.0	

### Industry

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		43	19.9	19.9	19.9
	1. Manufacturing	14	6.5	6.5	26.4
	2. Retail/wholesale	14	6.5	6.5	32.9
	3. Telecoms/IT	67	31.0	31.0	63.9
	4. Finance/ Insurance	42	19.4	19.4	83.3
	5. Healthcare	11	5.1	5.1	88.4
	7. Government	25	11.6	11.6	100.0
	Total	216	100.0	100.0	

**Table 3: Participation information**

## 6 DATA ANALYSIS & DISCUSSION

### 6.1 Measurement model

The component of the model known as the measurement model is the part of the model that investigates the links between measured and concealed variables.

In the model of the research that is now being given, reflective indicators are used in order to quantify each pick up variable. Validation of the measurement model is required, and the criteria for doing so include construct reliability and discriminate validity.

### 6.2 Construct Reliability

Dillon and Goldstein (1984) established AVE, which states that for LVs to be suitably convergent, their measures must account for more than 50% of explained or common variation in the factor analytic sense (with less than 50% error variance). The AVE for X when using  $x_1, x_2, \dots, x_n$  as indicators is:

$$\frac{\sum I_i^2 \text{Var}(x_i)}{\sum I_i^2 \text{Var}(x_i) + \sum \sigma_i^2}$$

The loading of variable  $x_i$  on variable X is denoted by  $I_i$  the variance of variable  $x_i$  is denoted by  $\text{Var}(x_i)$ , the measurement error of variable  $x_i$  is denoted by  $\sigma_i^2$ , and the symbol indicates (Fornell & Larcker, 1981). We eliminated IO5 and IO6 survey responses in the sake of improving AVE. As may be seen by comparing tables -3 and -, both conditions are met.

	Composite reliability (rho_c)
COM	0.776
ISC	0.889

<b>ISE</b>	0.854
<b>ISI</b>	0.856
<b>ISKS</b>	0.787
<b>PN</b>	0.781

**Table 4: AVE**

	<b>Average variance extracted (AVE)</b>
<b>COM</b>	0.634
<b>ISC</b>	0.729
<b>ISE</b>	0.667
<b>ISI</b>	0.666
<b>ISKS</b>	0.562
<b>PN</b>	0.657

**Table 4: Composite reliability**

### 6.3 Discriminate Validity

Table 11 shows the square root of AVE shown along the diagonal of the hidden variable correlation. The validity of our measuring approach is shown by the fact that these values are greater than the correlation between the respective constructs.

	<b>ATCI</b>	<b>ATT</b>	<b>COM</b>	<b>ICBI</b>	<b>ISC</b>	<b>ISE</b>	<b>ISI</b>	<b>ISKS</b>	<b>PN</b>
<b>ATCI</b>	1.000								
<b>ATT</b>	0.283	1.000							
<b>COM</b>	0.525	0.229	0.796						
<b>ICBI</b>	0.550	0.314	0.531	1.000					
<b>ISC</b>	0.689	0.472	0.726	0.480	0.854				
<b>ISE</b>	0.599	0.440	0.639	0.539	0.796	0.817			
<b>ISI</b>	0.671	0.504	0.756	0.569	0.883	0.885	0.816		
<b>ISKS</b>	0.476	0.810	0.530	0.434	0.651	0.620	0.673	0.750	
<b>PN</b>	0.555	0.501	0.415	0.798	0.493	0.595	0.720	0.412	0.811

**Table 5: Discriminate Validity**



## 6.4 F<sup>2</sup>

A test of independence using the F-squared statistic. Cohen (1988) suggests using the cutoffs of 0.02, 0.15, and 0.35 to differentiate between moderate and large impacts. Display the F2 result in table 12.

## 6.5 Structural model

In a nutshell, we may define a structural model as the interdependencies between unobservable factors. A structural model reveals the theoretical model's unobserved variables and the relationships between them.

## 6.6 Coefficient of determination (R<sup>2</sup>)

To evaluate the effectiveness of the structural model, we make use of the coefficient of determination (R<sup>2</sup>) as well as the significance levels of each route coefficient.

	R-square
ATT	0.824
ICBI	0.099

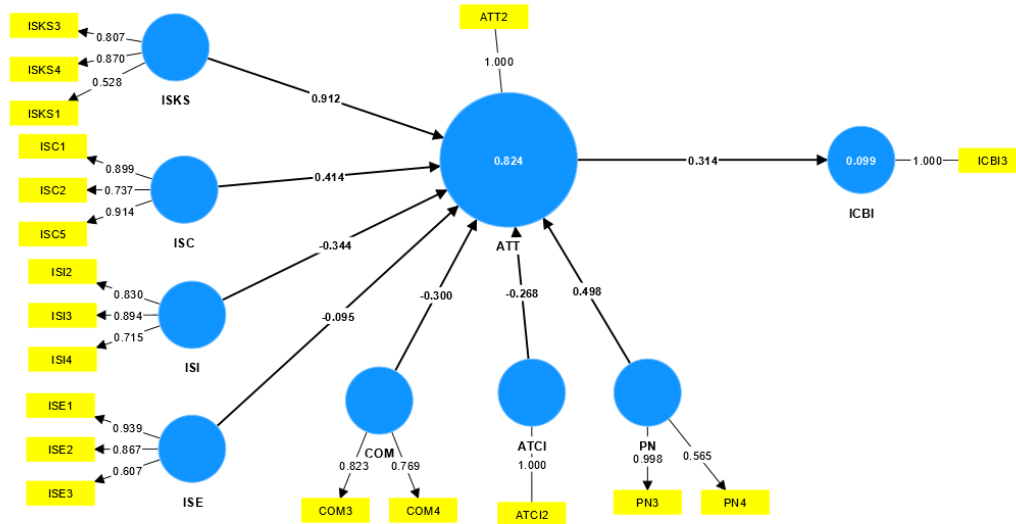
**Table 6: R<sup>2</sup>**

	Original sample (O)	T statistics ( O/STDEV )	Result
ATCI -> ATT	-0.268	4.059	Support
ATCI -> ICBI	-0.084	2.484	Support
ATT -> ICBI	0.314	3.697	Support
COM -> ATT	-0.3	4.057	Support
COM -> ICBI	-0.094	3.059	Support
ISC -> ATT	0.414	2.691	Support
ISC -> ICBI	0.13	2.272	Support
ISE -> ATT	-0.095	0.772	Support
ISE -> ICBI	-0.03	0.76	Unsupported
ISI -> ATT	-0.344	1.242	Unsupported
ISI -> ICBI	-0.108	1.128	Unsupported
ISKS -> ATT	0.912	18.249	Unsupported
ISKS -> ICBI	0.286	3.678	Support
PN -> ATT	0.498	7.183	Support

PN -> ICBI	0.156	3.257	Support
------------	-------	-------	---------

**Table 7: Hypothesis Testing**

## 6.7 Research result



**Figure 1: Final Diagram**

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics ( O/STDEV )	P values
ATCI → ATT	-0.268	-0.240	0.066	4.059	0.000
ATCI → ICBI	-0.084	-0.077	0.034	2.484	0.013
ATT → ICBI	0.314	0.310	0.085	3.697	0.000
COM → ATT	-0.300	-0.283	0.074	4.057	0.000
COM → ICBI	-0.094	-0.087	0.031	3.059	0.002
ISC → ATT	0.414	0.400	0.154	2.691	0.007
ISC → ICBI	0.130	0.123	0.057	2.272	0.023
ISE → ATT	-0.095	-0.096	0.123	0.772	0.440
ISE → ICBI	-0.030	-0.029	0.039	0.760	0.447
ISI → ATT	-0.344	-0.332	0.277	1.242	0.214
ISI → ICBI	-0.108	-0.103	0.096	1.128	0.259
ISKS → ATT	0.912	0.899	0.050	18.249	0.000
ISKS → ICBI	0.286	0.279	0.078	3.678	0.000
PN → ATT	0.498	0.486	0.069	7.183	0.000
PN → ICBI	0.156	0.151	0.048	3.257	0.001

Here the red-colored values are not accepted because P value must be less than 0.05 but here, the P values are greater than 0.05

## 6.8 Discussion

Incorporating the Social Bond Theory with the concept of engagement, this study is significant. Users are more likely to take information security seriously if they demonstrate

their involvement via the sharing of knowledge, collaboration, action, and learning from experience. There is a direct correlation between the amount of security breaches and the amount of education people have about information security (Akhunzada et al., 2015; Caputo et al., 2014). This is one of the first studies we are aware of that discusses ISOP compliance from the perspective of information security engagement. The new perspective on compliance behavior intentions with ISOP that results from this unified style of thinking is promising. We believe that this theoretically-oriented study contributes to the existing literature. The data analysis revealed that information security knowledge sharing significantly influences individuals' attitudes on adhering to ISOP. How individuals feel about ISOP compliance is influenced by how much they know and understand about information security, which may be improved via knowledge sharing. Similar findings were found by Rocha Flores et al. (2014) and Tamjidyamcholo et al (2014). Positive attitudes regarding ISOP compliance were shown to be significantly correlated with information security cooperation. The method in which individuals collaborate might account for this result. Collaborating on information security helps ensure that valuable data is safeguarded. Working together raises consciousness and provides invaluable experience, both of which influence how individuals feel about adhering to ISOP (Vroom and von Solms, 2004). Staff members may get knowledge about information security via intervention or other training approaches. When employees are aware of this, their attitudes about ISOP compliance in the realm of information security change (Albrechtsen and Hovden, 2010; Parsons et al., 2014). Evidence from this study also points to information security expertise as a factor in this kind of engagement. Employees' attitudes toward ISOP compliance are significantly impacted by their level of information security expertise (Rhee et al., 2009). The findings did not back up H5, as we had predicted; attachment did not have a substantial impact on ISOP compliance attitudes. One explanation for this result might be that everyone involved really does believe they are benefiting in some way (Casper and Harris, 2008). Reading the literature, we hypothesized that workers' commitment levels would have an impact on their attitudes on ISOP compliance. Those that are dedicated to their positions won't risk jeopardizing them. The statistical study revealed encouraging findings, revealing a correlation between individuals' levels of commitment and their levels of satisfaction with their efforts to adhere to ISOP. This confirms the findings of an Ifinedo investigation (2014). Employees' attitudes about complying with ISOP are most significantly influenced by personal norms, the final component of the framework to have an impact. Individuals' expectations of what they themselves should do in order to behave in accordance with ISOP become personal norms.

Individual norms were shown to have a significant impact on how individuals felt about adhering to ISOP. Van Niekerk and Von Solms's research confirmed this to be the case (2010). Finally, statistical testing revealed a correlation between individuals' subjective evaluations of ISOP and their intentions to actually implement the recommendations. This conclusion is consistent with those of previous investigations (Ifinedo, 2014; Siponen et al., 2014).

## 7 CONCLUSION, LIMITATIONS AND FUTURE WORK

Services, apps, information, and opportunities are now available online. Anecdotal and empirical data suggests that information security breaches are increasing in incidence and severity. Organizational information security breaches may be prevented by following rules and procedures (Ifinedo, 2014; Vance et al., 2012). This study uses social connection and participation theories to further research on how firms implement information security standards. Involvement, dedication, and beliefs impact employee compliance with information security rules and procedures. Attachment didn't affect workers' attitudes about information security rules. Information security involves knowledge exchange, cooperation, intervention, and experience.

Organizational information security knowledge sharing raises employee awareness and emphasizes compliance with rules and procedures. Intrinsic and extrinsic motives may help managers share information security expertise. Extrinsic motivation is external. Rewards often motivate extrinsically (Lai and Chen, 2014). (2014). Intrinsic motivation comes from enjoying the activity without external pressure or reward. Satisfaction and pleasure fuel intrinsic motivations (Shibchurn and Yan, 2015). Curiosity or self-worth may provide this pleasure (Wang and Hou, 2015). (KwangWook and Ravichandran, 2011). These motivators may help management increase information security knowledge sharing.

Information security cooperation also affects employee compliance with company information security policy. Collaborating to secure information assets is an example of collaboration. Organizational support may increase information security cooperation. Organizational support is how much the firm values and cares about its workers (Shropshire et al., 2015). Management may use this to increase information security cooperation.

This research reveals that management might help workers implement ISOP by fostering information security knowledge sharing and collaboration. Training staff well affects ISOP compliance. Training methods include formal presentations, posters, seminars, emails, websites, meetings, pens, and games. Information security requires proper training to raise awareness. This study found that information security experience strongly influences ISOP compliance attitudes. Information security experience derives from real-world practice. This deepens comprehension and transforms ISOP followers' attitudes.

In this research, attachment didn't affect ISOP followers' feelings.

Employee interest and advantage caused this disagreement. Management should foster organizational cohesiveness for information security. Talking about these problems at frequent group gatherings may help. Any company must take time to teach social norms and values. Socialization may help ISOP compliance.

Strong devotion to the organization's aims, rules, and laws involves protecting informational assets. Statistics show that dedication affects ISOP compliance. Organizational management may follow this. Employee values, views, and opinions are personal standards. Management should consider that personal norms may strongly influence organizational subjective norms.

This research didn't cover everything. This survey sampled Malaysian organizations with good information security procedures. Many firms lack information security procedures to prevent data breaches. Permission to survey and gather data in information security is difficult to get, but a larger sample size and more firms for research may increase generalization. Malaysia collected data. Other nations might use this. Another major issue is that the computerized questionnaire allows several answers. Controlling respondent IP addresses might alleviate these concerns. Thus, we can identify those who answered twice.

This study provides a testable research proposal. This research may examine how gender, age (teen, young adult, adult), education, employment style, and other factors impact how individuals obey organizational information security regulations. This area might also study organizational culture, trust, interpersonal and team traits, motivational variables, and rewards. This study's elements and other views might be used to generate complete and integrated ISOP compliance models for enterprises. Knowledge reduces information security breaches. Organizational learning perspectives may be a good ISOP-compliant study topic.

## 8 Questionnaire

Item	Description	Source
<b>Information security knowledge sharing</b>		
ISKS1	In an effort to lessen the danger of information security breaches at my workplace, I am very open about sharing the knowledge I have acquired in this area.	(Safa et al. 2016)
ISKS2	To stay current in the field of information security, I engage in knowledge exchange with other professionals.	
ISKS3	Sharing my expertise of information security with others has helped me	

	better appreciate the value of our company's practices in this area.	
ISKS4	In my opinion, one of the best ways to reduce the likelihood of data breaches is via the dissemination of existing expertise in the field of information security.	
ISKS5	In my opinion, it is beneficial for businesses to encourage the exchange of information security expertise.	
ISKS6	As a result of learning more about information security from others, I am more likely to adhere to relevant rules and practices.	
<b>Information security collaboration</b>		
ISC1	To work together with the data security group seems fair to me.	(Safa et al. 2016)
ISC2	Working with information security professionals has changed my perspective on following rules.	
ISC3	I believe that the information security events at my company have been reduced thanks to my cooperation with industry professionals.	
ISC4	I believe that the appropriate reaction to information security breaches is the result of my engagement with information security specialists.	
ISC5	Working with professionals, I am able to get in-depth expertise in the field of information security.	
<b>Information security intervention</b>		
ISI1	My knowledge of information security is more robust thanks to training sessions.	(Safa et al. 2016)
ISI2	My outlook on following information security rules changed as a result of the several information security training classes I've taken.	
ISI3	My outlook on following information security rules changed as a result of the many information security training approaches I underwent.	
ISI4	In my opinion, the training program is in line with the information security standards at my company.	
<b>Information security experience</b>		
ISE1	My perspective on following the company's information security policy has changed as a result of my work in the field of information security.	(Safa et al. 2016)
ISE2	Since I have worked in the field of information security, I am more likely to follow regulations in this area.	
ISE3	The information security field is always expanding my mind with new information.	
ISE4	In my opinion, the right actions are taken in response to information security issues because of my background in the field.	
<b>Attachment</b>		
ATT1	The issues of data breach and information security that my employer faces matter to me.	(Safa et al. 2016)
ATT2	I talk to my coworkers about why it's crucial to have strict standards in place to protect sensitive company data.	
ATT3	I value the feedback of my coworkers as we formulate our information security policy for the company.	
ATT4	When it comes to maintaining a safe workplace, I always adhere to established regulations and procedures.	
<b>Commitment</b>		
COM1	I will do all in my power to protect sensitive data.	(Safa et al. 2016)
COM2	I dedicate a lot of time and effort to ensuring the effectiveness of our company's information security policy.	
COM3	I will actively advocate for my company's information security initiatives.	

COM4	I make it a point to refresh my knowledge whenever there are changes to our company's information security procedures.	
<b>Personal norms</b>		
PN1	The rules and regulations set out by my company's information policies cannot be disregarded.	(Safa et al. 2016)
PN2	The company takes violations of its information security standards very seriously.	
PN3	My company has strict information security regulations that must be adhered to at all times.	
PN4	Policy adherence in the realm of information security is crucial.	
<b>Attitude toward compliance with ISOP</b>		
ACI1	A commitment to ISOP compliance is required.	(Safa et al. 2016)
ACI2	It's in your best interest to adhere to ISOP.	
ACI3	By sticking to ISOP, you may lessen the likelihood of any security flaws occurring.	
ACI4	To abide with ISOP is wise.	
<b>ISOP compliance behavioral intentions</b>		
ICBI1	Definitely, I will follow ISOP guidelines.	(Safa et al. 2016)
ICBI2	I plan to keep following ISOP guidelines.	
ICBI3	To safeguard corporate knowledge, I shall follow ISOP's guidelines.	
ICBI4	In the future, I anticipate adhering to ISOP.	
ICBI5	Each time it is practical, I shall adhere to ISOP.	

## 9 References

- Abdullah Al Mamun, J. B. (2021). Cyber Security Awareness in Bangladesh: An Overview of Challenges and Strategies. *International Journal of Computer Science and Information Technology Research*, 9(1), 88-94. Retrieved from <https://www.researchpublish.com/upload/book/paperpdf-1611555745.pdf>
- Agarwal, C. L. (2010). Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, 34(3), 613-643. doi:10.2307/25750694
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211. doi:10.1016/0749-5978(91)90020-T
- Akmarlsmail, N. S. (2013). A customer loyalty formation model in electronic commerce. *Economic Modelling*, 35, 559-564.
- Alain Chong, Y.-L. a.-B. (2015). Predicting RFID adoption in healthcare supply chain from the perspectives of users. *International Journal of Production Economics*, 159, 66-75.



- Angela Sasse and Sacha Brostoff, a. D. (2004). Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal*, 19, 122-131. doi:10.1023/A:1011902718709
- Aronson E, T. D. (2010). *Social psychology*. Retrieved from <https://www.amazon.com/Social-Psychology-9th-Elliot-Aronson/dp/0133936546>
- Aronson, E. W. (2010). *ocial Psychology*. 7th Edition,. *Pearson Prentice Hall*.
- Bandura. (1977). Self-efficacy: toward a unifying theory of behavioral change. *84*(2), 191-215. doi:10.1037//0033-295x.84.2.191
- Bandura, A. (1991). Social cognitive theory of self-regulation. *Organizational Behavior and Human Decision Processes*, 50(2), 248-287. doi:[https://doi.org/10.1016/0749-5978\(91\)90022-L](https://doi.org/10.1016/0749-5978(91)90022-L)
- bangla, B. n. (2021). *Bangladesh Bank Reserve Heist: How North Korean Hackers Made Off Almost a Billion Dollars*. BBC NEWS BANGLA. Retrieved from <https://www.bbc.com/bengali/news-57549877>
- Baharin, S. H. (2019). *Issues and Trends in Information Security Policy Compliance*. doi:10.1109/ICRIIS48246.2019.9073645
- Burbidge, T. (2021). *Cybercrime thrives during pandemic: Verizon 2021 Data Breach Investigations Report*. Retrieved from <https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report>
- Burcu Bulgurcu, H. C. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, 34, 523-548. doi:10.2307/25750690
- Chan, M. a. (2005). Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy and Security*, 1, 18-41. doi:10.1080/15536548.2005.10855772
- Chong, F. T. (2012). A SEM–neural network approach for understanding determinants of interorganizational system standard adoption and performances. *Decision Support Systems*, 54(0167-9236), 621-630. doi:<https://www.sciencedirect.com/science/article/pii/S0167923612002059>
- Clay Posey, T. L. (2015). The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. *Journal of Management Information Systems*, 32(4), 179-214. doi:10.1080/07421222.2015.1138374
- Cohen, E. (1988). Authenticity and commoditization in tourism. *Annals of Tourism Research*, 15(3), 371-386. doi:[https://doi.org/10.1016/0160-7383\(88\)90028-X](https://doi.org/10.1016/0160-7383(88)90028-X)
- Cornelia Pechmann and Guangzhi Zhao and Marvin Goldberg, a. E. (2003). What to Convey in Antismoking Advertisements for Adolescents: The Use of Protection Motivation Theory to Identify Effective Message Themes. *The Journal of Marketing*, 67, 1-18. doi:10.1509/jmkg.67.2.1.18607
- Foster, A. R. (2020). Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study. *Computers in Human Behavior*, 108(0747-5632), 106319. doi:<https://doi.org/10.1016/j.chb.2020.106319>

- Gerald V. Post, A. K. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security*, 26(3), 229-237. doi:<https://doi.org/10.1016/j.cose.2006.10.004>
- Ginther, M. G. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, 73(0167-4048), 345-358. doi:<https://doi.org/10.1016/j.cose.2017.11.015>
- Haykin, S. (2001). Neural networks. *A comprehensive foundation*.
- Herath, T. a. (2014). Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information Systems Journal*, 24(1), 61–84. doi:<https://doi.org/10.1111/j.1365-2575.2012.00420.x>.
- Herawan, N. S. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, 53(0167-4048), 65-78. doi:<https://doi.org/10.1016/j.cose.2015.05.012>
- Hew, J.-J. S.-H.-B.-S. (2014). Understanding and predicting the motivators of mobile music acceptance – A multi-stage MRA-artificial neural network approach. *Telematics and Informatics*, 31(4), 569-584. doi:<https://doi.org/10.1016/j.tele.2013.11.005>
- Higgins, D. R. (1995). Computer Self-Efficacy: Development of a Measure and Initial Test. *Management Information Systems*, 19(2), 189-211. doi:<https://doi.org/10.2307/249688>
- Hsu, B. K.-H. (2003). An Investigation of Volitional Control in Information Ethics. *Behaviour & Information Technology - Behaviour & IT*, 22, 261-270. doi:10.1080/01449290301781
- Iacobucci D, C. G. (2009). Marketing research: methodological foundations (with Qualtrics Card). 10th. ed.
- Ifinedo, P. (2009). An Exploratory Study of the Relationships between Selected Contextual Factors and Information Security Concerns in Global Financial Services Institutions. *Journal of Information Privacy and Security*, 25-49.
- Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83-95. doi:<https://doi.org/10.1016/j.cose.2011.10.007>
- Jeffrey D. Wall, M. W. (2017). To fear or not to fear? A critical review and analysis of fear appeals in the information security context. *Communications of the Association for Information Systems*, 41(3). doi:<https://doi.org/10.17705/1CAIS.04113>
- John Cacioppo, R. P. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. 153, 177.
- Johnston Allen, W. M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. 34(3), 549-566. doi:10.2307/25750691
- Jolton, J. M. (2005). Analysis of end user security behaviors. *Computers & Security*, 24(2), 124-133. doi:<https://doi.org/10.1016/j.cose.2004.07.001>
- Julian Jang-Jaccard, S. N. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973-993. doi:<https://doi.org/10.1016/j.jcss.2014.02.005>

- Kamrul Faisal. (2022). *The problem with Bangladesh's data protection framework and its solutions*. Dhaka: 2022. Retrieved from <https://www.tbsnews.net/thoughts/problem-bangladeshs-data-protection-framework-and-its-solutions-480030>
- Knapp, K. a. (2006). Information security: Management's effect on culture and policy. *Information Management Comput. Security*, 14, 24-36. doi:10.1108/09685220610648355
- Kreie, L. N. (2004). What influences IT ethical behavior intentions-planned behavior, reasoned action, perceived importance, or individual characteristics? *Information & Management*, 42(1), 143-158. doi:<https://doi.org/10.1016/j.im.2003.12.008>
- Kurnia, I. M. (2017). To use or not to use: Modelling end user grumbling as user resistance in pre-implementation stage of enterprise resource planning system. *Information Systems*, 69(0306-4379), 164-179. doi:<https://doi.org/10.1016/j.is.2017.05.005>
- Larcker, C. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, 18(1), 39-50.
- Larsen, Y. L. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, 18(2), 177-187. doi:10.1057/ejis.2009.11
- Mahmood, S. P. (2007). Employees' Behavior towards IS Security Policy Compliance. *40th Annual Hawaii International Conference on System Sciences*, 156b-156b.
- Mark Chan, a. I. (2005). Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy and Security*, 1, 18-41. doi:10.1080/15536548.2005.10855772
- Mark Chan, I. W. (2005). Perceptions of information security at the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security*, 1(3). doi:10.1080/15536548.2005.10855772
- Mutlaq Alotaibi, S. F. (2016). *Information security policies: A review of challenges and influencing factors*. 2016. doi:10.1109/ICITST.2016.7856729
- Myry, L. a. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, 18. doi:10.1057/ejis.2009.10
- Nader Sohrabi Safa, M. S. (2015). Information security conscious care behavior formation in organizations. *Computers & Security*, 53, 65-78. doi:<https://doi.org/10.1016/j.cose.2015.05.012>
- Negnevitsky, M. (2005). *Artificial intelligence: a guide to intelligent systems*.
- Ooi, L.-Y. L.-S.-H.-B. (2013). Predicting the determinants of the NFC-enabled mobile credit card acceptance: A neural networks approach. *Expert Systems with Applications*, 40(14), 5604-5620. doi:<https://doi.org/10.1016/j.eswa.2013.04.018>
- Ooi, L.-Y. L.-S.-H.-B. (2013). Predicting the determinants of the NFC-enabled mobile credit card acceptance: A neural networks approach. *Expert Systems with Applications*, 40(14), 5604-5620. doi:<https://doi.org/10.1016/j.eswa.2013.04.018>

- P A Rippetoe, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *52*(3), 596-604. doi:10.1037//0022-3514.52.3.596
- P A Rippetoe, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology*, *52*(3), 596-604. doi:10.1037/0022-3514.52.3.596
- Philip M Podsakoff, S. B.-Y. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*. *88*(5). doi:10.1037/0021-9010.88.5.879
- Philip Menard, G. J. (2017). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. *Journal of Management Information Systems*, *34*(4), 1203-1230. doi:https://doi.org/10.1080/07421222.2017.1394083
- Rao, T. H. (2009a). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, *18*, 106-125. doi:10.1057/ejis.2009.6
- Rao, T. H. (2009b). Encouraging information security behaviors: role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165. doi:10.1016/j.dss.2009.02.005
- Robert E. Crossler, A. C. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90-101. doi:https://doi.org/10.1016/j.cose.2012.09.010
- Robert Larose, N. J. (2008). Promoting Personal Responsibility for Internet Safety. *Commun. ACM*, *51*, 71-76. doi:10.1145/1325555.1325569
- Rogers R W, a. J. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. *In book: Social Psychophysiology*, 153-177.
- Sheela, K. G. (2013). Review on Methods to Fix Number of Hidden Neurons in Neural Networks. *Mathematical Problems in Engineering*. doi:10.1155/2013/425740
- Sheela, K. G. (2013). Review on Methods to Fix Number of Hidden Neurons in Neural Networks. *Mathematical Problems in Engineering*. doi:10.1155/2013/425740
- SHEINA, M. S. (2000). Prediction and intervention in health-related behavior: a meta-analytic of protection motivation theory. *Journal of Applied Social Psychology*, *30*(1), 106-143. Retrieved from <http://repository.essex.ac.uk/12706/#:~:text=Protection%20motivation%20theory%20%28PMT%29%20was%20introduced%20by%20Rogers,have%20been%20the%20subject%20of%20a%20meta-analytic%20review.>
- Sipone, A. V. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly: Management Information Systems*, *34*, 487-502. doi:10.2307/25750688
- Siponen, P. P. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, *34*(4), 757-778. doi:https://doi.org/10.2307/25750704

- Sobers, R. (2022). *15 influential cybersecurity statistics and facts*. Retrieved from <https://www.varonis.com/blog/cybersecurity-statistics>
- Stanton, S. M. (2015). Behavioral information security. *Human-Computer Interaction and Management Information Systems: . Human-Computer Interaction and Management Information Systems*, 262-280.
- Straud, M. W. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), 2799-2816. doi:<https://doi.org/10.1016/j.chb.2008.04.005>
- Venkatesh, V. a. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 425-478. doi:10.2307/30036540
- Warkentin, A. C. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, 34, 549-566. doi:10.2307/25750691
- Willison, M. S. (2009). Information security management standards: Problems and solutions. *Information & Management*, 46(5), 267-270. doi:<https://doi.org/10.1016/j.im.2008.12.007>
- Xiaofeng Chena, D. W. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management*, 55(8), 1049-1060. doi:<https://doi.org/10.1016/j.im.2018.05.011>
- Xu, B.-Y. N. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46, 815-825. doi:<https://doi.org/10.1016/j.dss.2008.11.010>
- Younghwa Lee, K. A. (2005). Investigating Factors Affecting the Adoption of Anti-Spyware Systems. *Communications of the ACM*, 48(8), 72-77. doi:10.1145/1076211.1076243
- Younghwa Lee, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems. Journal of Information Systems*, 18(2), 177-187. doi:10.1057/ejis.2009.11
- Zhai, L. C. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, 39(0167-4048), 447-459. doi:<https://doi.org/10.1016/j.cose.2013.09.009>

# PLAGIARISM REPORT



Project Report Library  
to me, Imran ▾

11:23 AM (2 hours ago) ☆ ↶ ⋮

Dear Student,

Your Plagiarism Result is 26% for details Please see the attachment file.

**Please read the instruction:**

- **Report to be arranged according to the Page Numbering:**
  - a. Preliminary pages must be in lower case roman numerals e.g. i, ii, iii.
  - b. All pages of the main body or from chapter one will be numbered in Arabic numerals e.g. 1, 2, 3.
  - c. All pages have to be arranged according to the table of contents
- 2. **Format:** The report should be in **ONE FILE** and **PDF** document.
- 3. **Copyright Note:** Write ©**Daffodil International University** at footer
- For Library Clearance please fill up your information in Internship Portal. Five fields must be completed as like- ID, Name, Department, Project/Internship Title & Supervisor Name.  
[http://internship.daffodilvarsity.edu.bd/index.php?app=applicant\\_login](http://internship.daffodilvarsity.edu.bd/index.php?app=applicant_login)
- **Please attach the supervisor & your signature in the Approval and Declaration page.**
- When you send us a new document, just send a reply to all. Don't create/send new mail.
- **If needed please contact the following Officer**
- Badhan Hubert Corraya-01981323203, Md. Mostafizur Rahman-01847334818, Ms. Umme Ahasan-01847334816, Md. Dulal Uddin: 01847334802, Ms. Syeda Aklima-01713493041

**Daffodil International University Library:**  
Daffodil Smart City, Ashulia, Savar,  
Dhaka – 1341, Bangladesh