Daffodil International University

Thesis Paper

On

"Mathematical modelling of information security policy compliance: An integration of the theory of planned behavior and the protection motivation theory."

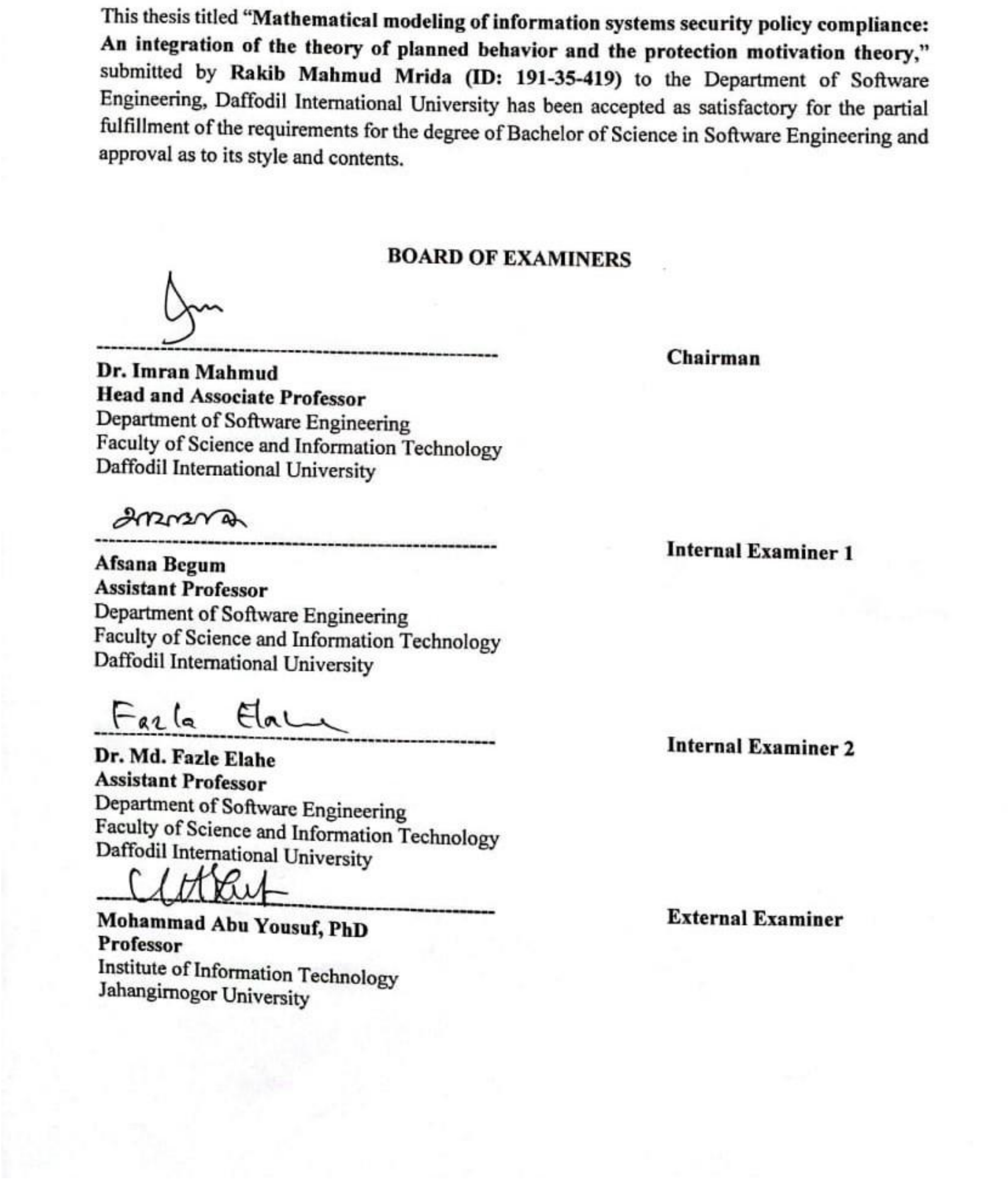
Supervised By

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

Submitted By

Rakib Mahmud Mrida
ID: 191-35-419
Batch: 28th
Department of Software Engineering
Daffodil International University

APPROVAL



This thesis titled **"Mathematical modeling of information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory,"** submitted by **Rakib Mahmud Mrida (ID: 191-35-419)** 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

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

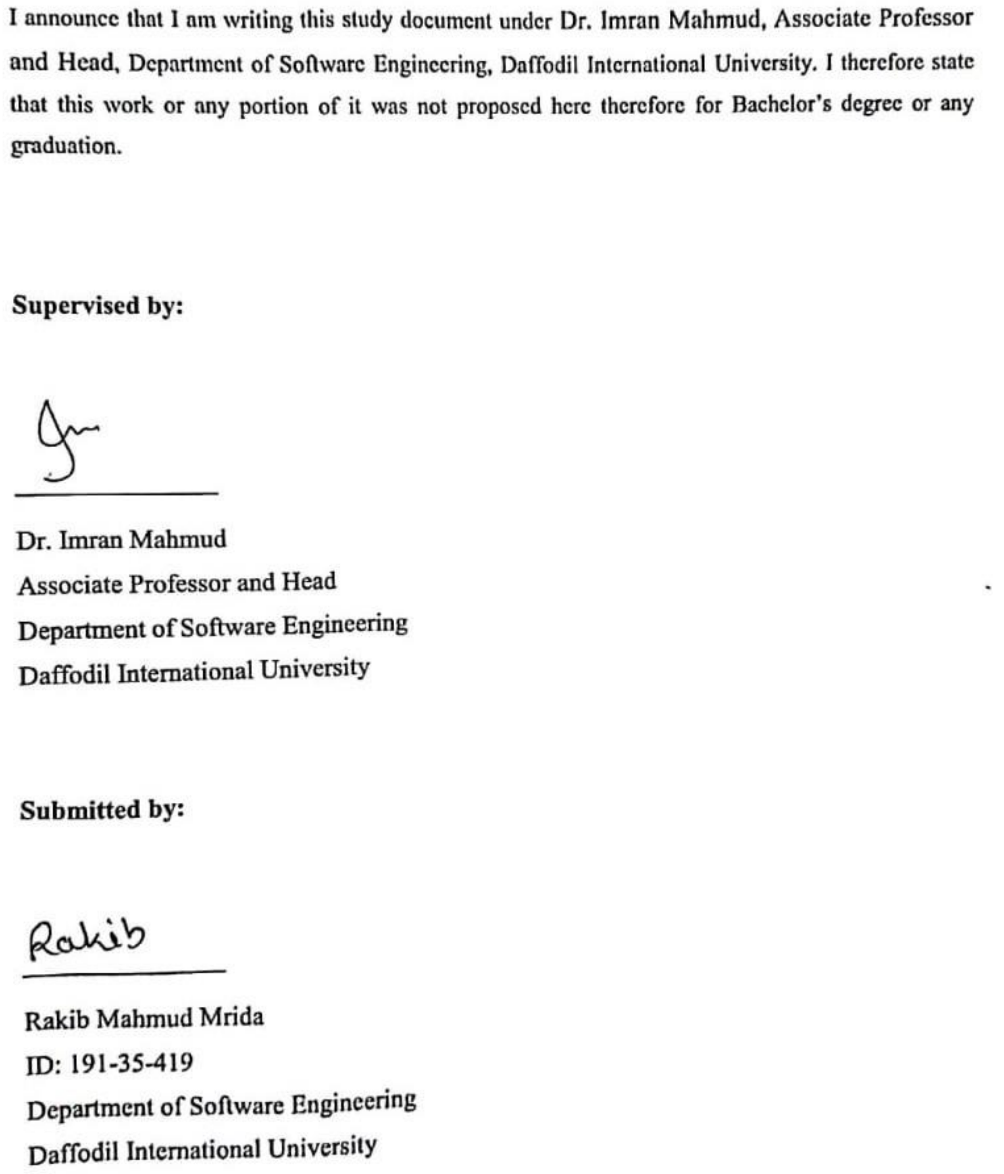
Afsana Begum — **Internal Examiner 1**
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Fazla Elahe

Dr. Md. Fazle Elahe — **Internal Examiner 2**
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Mohammad Abu Yousuf, PhD — **External Examiner**
Professor
Institute of Information Technology
Jahangirnogor 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:

Rakib

Rakib Mahmud Mrida
ID: 191-35-419
Department of Software Engineering
Daffodil International University

ACKNOWLEDGEMENT

First and foremost, I express my sincere gratitude to Almighty Allah for granting me the opportunity to finish this thesis.

Then I would like to thank my supervisor, Dr Imran Mahmud, Associate Professor and Head of the Department of Software Engineering at Daffodil International University, Bangladesh. I am incredibly grateful and indebted to him for his expert, sincere and valuable guidance and encouragement extended to me. My supervisor used his extensive knowledge and deep interest in artificial neural networks and partial least squares to complete this thesis. This endeavour was made possible by his never-ending patience, academic leadership, persistent encouragement, constant and vigorous supervision, constructive criticism, insightful counsel, reading numerous subpar versions, and fixing them at all levels.

I sincerely thank the other professors, teachers and employees of Daffodil International University's Software Engineering department. I also want to express my gratitude to everyone who participated in the survey for this thesis project. With their enthusiastic involvement and feedback, the validation survey was carried out satisfactorily.

Last but not least, I want to express my gratitude to my parents for their unwavering love and support. Without them, I would not have made it this far.

LIST OF ABBREVIATIONS

ISSP	=	Information system security policy
TPB	=	Theory of planned behavior
PMT	=	Protection motivation theory
IS	=	Information security
AVE	=	Average Variance Extracted
CR	=	Composite Reliability
LV	=	Latent Variable
PLS	=	Partial Least Squares
ANN	=	Artificial neural networks

Mathematical modelling of information security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory

Rakib Mahmud Mrida[a]

[a]*Department of Software Engineering, Faculty of science and information technology, Daffodil International University, Bangladesh*

KEYWORDS

Information systems security policy,
Behavioral intentions,
Policy compliance,
Theory of planned behavior,
Protection motivation theory

ABSTRACT

Information security (IS) is subject to increasing dangers as technology is increasingly integrated to connect and share data with other devices and systems through the Internet. By safeguarding IS as a key information and intelligence asset, organizations may thereby gain a competitive edge. The theory of planned behavior (TPB) and the protection motive theory were two important theories that were used in this study to evaluate information systems security policy (ISSP) compliance (PMT). The proposed and approved research model combined elements of the aforementioned ideas. In order to test the conceptualization of the research, relevant hypotheses were generated. Two-stage analytical method (PLS and ANN technique) for hypothesis testing and validation of the proposed model. In the initial step, this thesis will create some hypotheses. Then drawing those relationships with a box and arrow. After that, it will test whether those relationships are significant with some additional analysis. PLS can test the hypothesized relationships. In the second step, ANN modeling will validate the PLS result. This will set the priority of each significant relationship so that this study will quickly determine the ISSP compliance behavioral intention. This study will use ANN because it performs traditional tools in detecting linear and non-linear relationships rather than just linear ones. This thesis demonstrated that variables like self-efficacy, attitude toward compliance, subjective norms, response efficacy, and perceived vulnerability positively influence employees' intentions to comply with ISSP behavioral standards. It did this by surveying 114 business managers and IS professionals. The data analysis as indicators of ISSP behavioural compliance intentions did not support perceived severity and response costs. There is a discussion of the study's ramifications for both research and practice.

TABLE OF CONTENTS

LIST OF FIGURE

LIST OF TABLE

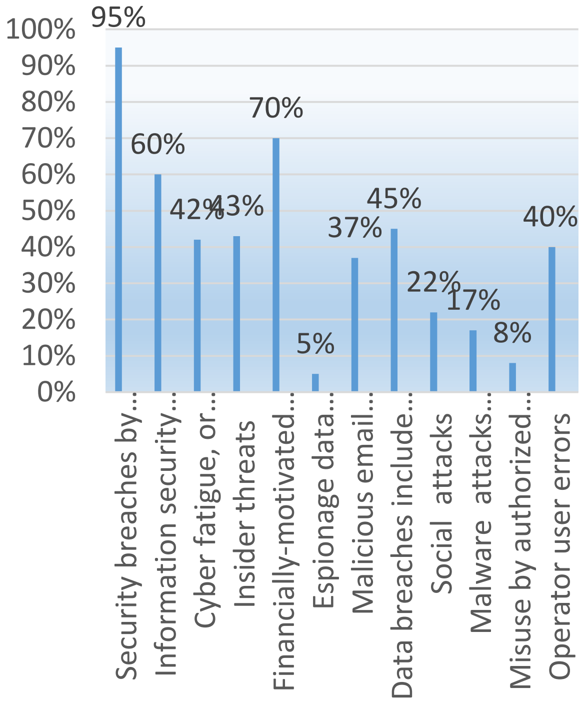
1 INTRODUCTION

1.1 Background

Information systems (IS) are essential to the sustainability of modern businesses because they frequently include vital organizational data resources (Ifinedo, 2009). Security is not limited to cryptography, secure data sharing, and privacy assurance but also refers to the protective behavior of security personnel. Access to organizational databases containing sensitive personal information and commercially important data is controlled by a highly effective authentication and authorization system (AkmarIsmail, 2013). Organizations often use a variety of tools and technical measures, such as installing firewalls, installing and updating anti-virus software, backing up systems, maintaining access controls, restricting, using encryption keys, using surge protectors, and thorough monitoring systems. In used to protect critical IS assets contained in such systems from misuse, abuse, and destruction (Larsen, 2009). However, the tools and dimensions mentioned above serve to provide a technical or technological solution to the problem and are not sufficient in providing full protection of IS organizational resources. (Rao T. H., 2009a). Researchers including (Jolton, 2005), and (Mahmood, 2007) noted that organizations can achieve greater success in securing there IS assets and resources if they focus on both technical and non-technical methods to do so. Therefore, it is incumbent on organizations to implement a multifaceted strategy to secure their IT resources and assets (Rao T. H., 2009b**).** Indeed, a number of studies have shown that firms that want to protect their IS resources view socio-organizational imperatives as being equally crucial (Burcu Bulgurcu, 2010). Organizational information security increasingly depends on the actions of IS professionals who are skilled in the collection, analysis, and use of data and are responsible for protecting access to user-accessible data (Julian Jang-Jaccard, 2014) (Clay Posey, 2015) . (Nader Sohrabi Safa, 2015)Reported that a primary reason for IS security lapses is the fact that IS professionals are the most vulnerable link in the security chain. These services are essential, but they pose a significant threat to your organization. For example, a study evaluating the trade-off between computer security and access concluded that employees are more likely to bypass security measures to complete their tasks (Gerald V. Post, 2007). Against this background, it is a useful approach for the organization to look at the intentions and actions of employees.

1.2 Problems around the world

Information leakage has become a severe problem for information security in the era of Industry 4.0 (IR 4.0). Data leakage in different organizations for different reasons is a threat to every organization. Incidents with information security are an issue caused by the conduct of individuals. Human mistake is more likely to result in data-leaking situations since humans create and maintain technology. Therefore, to ensure they are correctly understood, organizations must develop a data protection policy consensus among them (Bhaharin, 2019). During the internet era's beginning, cyber and information security (CIS) issues began to surface rapidly (Xiaofeng Chena, 2018). Information security (IS) is the current direction in today's digital environment. Due to phishing operations, organizations are threatened and in danger of being attacked online. Despite its immense relevance, the cybersecurity issue is dynamic and has not received much attention (Foster, 2020). Humans are particularly vulnerable to cyber threats because they are the weakest link (Ginther, 2018). To avoid cybercrimes like phishing and malware assaults on security systems that occur from human interaction, poor and risky security practices among employees in a business should be discovered, and mitigating measures like ongoing education and awareness are required. The most significant threat comes from end users for personal use or within enterprises (Philip Menard, 2017). Because it depends more on human mistakes than technological flaws, social engineering is still one of the most hazardous hacking methods cybercriminals use. This makes these attacks even more challenging because it's simpler to con people than to get past security measures. Hackers are aware of this: 85% of all data breaches involve human interaction, according to Verizon's Data Breach Investigations report (Burbidge, 2021). (Sobers, 2022)reports that most cybersecurity breaches are caused by human error. Below are some statistics on policy compliance issues around the world in 2022:



- Security breaches by human error (95%).
- Information security risk increasing (60%).
- Cyber fatigue, or apathy to proactively defending against cyberattacks (42%).
- Insider threats (43%).
- Financially-motivated data breaches approximately (70%).
- Espionage data breach (5%).
- Malicious email attachment (37%).
- Data breaches include hacking (45%).
- Social attacks (22%).
- Malware attacks include (17%).
- Misuse by authorized users (8%).

Fig 1: Security compliance issues around the world

1.3 Problem in Bangladesh

(Kamrul Faisal, 2022)Reported that Existing laws in Bangladesh fail to set standards to prevent the misuse of personal data. The numerous already documented privacy violations that occur every day in Bangladesh support this claim. Protection of privacy is a human right under the legal system of Bangladesh. In addition, unethical activities create unnecessary costs associated with cybercrime, undermine national integrity, and create distrust in e-services. For example, between March and October 2016, an official of Bangladesh Bank, a well-known bank in Bangladesh, fell into the trap of a phishing link. As a result, North Korean hackers could transfer $81 million from Bangladesh's central bank in 2016 (bangla, 2021). In addition, these actions have had serious consequences for the organization, including financial loss, reputational damage, and alleged personal privacy violations. Additionally, these actions have had serious consequences for the organization, including financial loss, reputational damage, and accusations of privacy violations, such as the hacking of Bangladesh by Turkish hackers. An Air Force website compromised the identities of 19 administrators in 2013. Facebook also compromised the data of 3 million Bangladeshi citizens in 2022 (Kamrul Faisal, 2022). Therefore, it is a useful approach for organizations to focus on the emergence of behavioral information security as the behaviors of organizational members that affect the availability, confidentiality, and integrity of information security (Robert E. Crossler, 2013) (Stanton, 2015).

1.4 Research Problem Statement

Despite the importance of protecting an organization's information assets with the help of IS experts, there is little research on information security protection in Bangladesh. Most of the research on this topic is limited to Western organizations. To what extent their information security argument can be generalized to Bangladesh, which has a very different cultural and institutional context, remains to be seen. Information comprehension system conformity with the security policy of various organizations in Bangladesh is the focus of the article. Bangladesh is now adopting ICT and expanding the use of ICT and the Internet greatly. Recent studies have emerged to explain the relationship between organizational rules, policies, and regulations outlined in an organization's information system security policy (ISSP) and employee compliance requirements as a useful process for formulating their information system security policy (ISSP) or the uses of organizational IS resources affects how staff members behave (Burcu Bulgurcu, 2010) (Ifinedo, 2009). The same body of literature shows that employees often do not readily follow such documents when such ISSPs exist to protect IS assets from abuse, misuse, and destruction (Sipone, 2010). Therefore, research intended to advance understanding of the difficulties that may arise, including hindering or promoting adherence to ISSPs in organizations, is welcome in the existing literature. Insights into this research area are beginning to emerge in the relevant literature (Burcu Bulgurcu, 2010) (Willison, 2009) (Agarwal, 2010).

To improve our understanding of ISSP compliance by workers in contemporary firms, two pertinent theories—the theory of planned behavior (TPB) (Ajzen, 1991) and the protection motive theory (PMT)) (Rogers R W, 1983) —will be combined. Research frameworks that included various theories with PMT and TPB have been employed in earlier publications (Burcu Bulgurcu, 2010) (Mahmood, 2007). To the best of my knowledge, no previous study has combined the two hypotheses. According to (Agarwal, 2010)Anderson and Agarwal's (2010) analysis of the literature in this field, ISSP compliance research has used the two aforementioned theories. (Sipone, 2010) said that ISSP compliance research employing fear appeal theories frequently do not always explain noncompliance behaviors with regard to the PMT, which highlights the fear appeal perspective. Others gave support for the viewpoint held by (Sipone, 2010) (Rao T. H., 2009b). This research intends to further our understanding of the field by fusing the PMT with the TPB, an enduring behavior-intention theory. Additionally, compliance is a complicated topic, and it should be investigated from various angles to advance understanding (Aronson E, 2010).

Research in this paper demonstrates that by incorporating PMT with TPB, we can build our knowledge in this area or examine the effects of integrated PMT and TPB theories on compliance information security behavioral intentions. They concluded that their situation could have been improved in understanding the data principles used in current guidelines, such as investigating Using qualitative techniques and ISSP behavioral compliance such as in-depth surveys and focus groups to enrich insights. These organizations need a deep understanding of cybersecurity issues. These organizations need a deep understanding of cybersecurity issues. This present research is designed needs to be better-clarified problems, and the situation needs to be analyzed for ways to overcome the challenges and complete the growing body of knowledge in this field.

1.5 Research Question

RQ: Does using the Protection motivation theory and theory of planned behavior (all the variables) influence information system security policy compliance?

1.6 Research Objective

RO: To test the effect of integrated PMT and TPB theory on compliance information security behavioral intention.

1.7 Organization of the chapter

The remainder of this article is organized as follows to further discuss the thesis. Chapter 2: Literature review, which reflects previous works on information system security behavioral intentions and also discusses the research gaps. After Chapter 2 i.e., in Chapter 3, we have written about Research Model and Hypothesis. Chapter 3, followed by Chapter 4 we have discussed the research methodology ie data collection procedure, demographic information, and data analysis techniques, and we have written about sample size and population, measurement items, and data analysis techniques. In Chapter 5, following Chapter 4, we have explained the results of the data analysis. I have discussed the results in chapter 6. In chapter 7, we have mentioned the conclusion; in chapter 8, we have mentioned the survey questions; and in chapter 9, we have added references.

2 LITERATURE REVIEW

IT organizations in Bangladesh employ many information systems and face many threats to information security, thus providing an excellent context for information security research. Until now, research in the Bangladeshi thesis has only briefly explored perceptions of cyber security awareness. In order to exercise formal social control, ISIS fails to define security fully. This is consistent with previous research examining IS violations in the context of rational choice (Abdullah Al Mamun, 2021). Concerning the PMT, which highlights the perspective of fear appeal. According to (Sipone, 2010)ISSP compliance research that uses fear appeal theories to explain noncompliance behaviors frequently falls short. Others provide confirmation for the viewpoint held by (Sipone, 2010). Given that this beneficial effect is shown in work satisfaction, it is likely that more contented IS professionals conduct information security-related tasks in their roles in accordance with the corporate information security standards that IT businesses demand and anticipate. According to the social exchange theory, people are more likely to commit themselves to engage in positive organizational behaviors if they are happy and believe that their employment relationship is one of reciprocal exchange, has been shown to be the foundation for the correlation between levels of job satisfaction and performance (Zhai, 2013) (Philip M Podsakoff, 2003). Questionnaire questions were randomly ordered, and different scales were used to reduce floor effects that could induce uniform responses from participants. In addition, statistical procedures. Harmon's univariate test was used to assess whether such biases were indeed a sampling problem (Philip M Podsakoff, 2003). For instance, self-efficacy and the adopting-spyware software were found to have a direct, positive link (Warkentin, 2010). Similar findings were made by other researchers, who discovered a link between perceptions toward a home wireless network's security and self-efficacy (Agarwal, 2010) (Mark Chan a. I., 2005). Although the direction of the link is in line with expectations and findings from other studies (Larsen, 2009) (Straud, 2008), the relationship's strength is insufficient to support the stated hypothesis. Response cost did not significantly affect compliance intentions, according to research similar to the one given here (Rao T. H., 2009a) that looked at the impact of response cost on ISSP behavioral compliance. This thesis discovered that intentions for protective behavior are significantly influenced by how well coping strategies are perceived (i.e., response cost and self-efficacy). The implications of response cost and self-efficacy on IS policy compliance intention as well as users' behavioral intents to utilize email authentication systems, have been examined in previous studies (Rao T. H., 2009b) (Sipone, 2010); (Herath, 2014) . To avoid the floor effect, which could cause participants to give repetitive answers, the questionnaire's questions were randomly assigned to different scales. Additionally, the Harmon one-factor test was employed to determine whether these biases were actually a problem in our sample (Philip M Podsakoff, 2003). In our data, one factor may account for 25.3% of the covariance, demonstrating that CMV was not a problem. To determine whether non-response bias occurred in our data, we contrasted early and late respondents from the mail-in and online surveys (Iacobucci D, 2009). For instance, the study by (Burcu Bulgurcu, 2010) and (Rao T. H., 2009a) that studied ISSP behavioral compliance by employees with TPB, PMT, and other theories modeled concern levels and attitude as modifiers of the connection between perceived severity and ISSP behavioral compliance. Such a paradigm might offer a different understanding of the outcome than what was found here. The study has its drawbacks. Although common technique bias was not an issue for this study, it is still possible that participants may have responded to some of the topics under investigation in a way that was "socially desirable" (Philip M Podsakoff, 2003). Such things must be considered to improve insight (Younghwa Lee K. A., 2005). The results of this study lend more credence to previous research that showed the impact of self-efficacy, reaction efficacy, social norms, compliance attitude, and perceived vulnerability on employees' ISSP behavioral compliance. For instance, focused security education and training initiatives should emphasize the significance of information security protection and outline the employees' need to do so (Siponen, 2010). This is supported by an earlier study, which discovered that whenever organization managers instill fear in their information security subordinates, those individuals solidify their identities as guardians of corporate information security (Jeffrey D. Wall, 2017). The largest covariance explained by one factor in the data was 25.3%, indicating that CMV was not a problem in the data. We compared early and late respondents to email and online surveys to assess whether non-response bias was present in the data (Iacobucci D, 2009).

3 THEORETICAL BACKGROUND

Protection Motivation Theory (PMT), which was developed by (John Cacioppo, 1983) enhanced the health-related belief model in the social psychology and health domains with the creation of the Protection Motivation Theory (PMT) (P A Rippetoe, Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat, 1987) (SHEINA, 2000). In order to better understand how fear appeals work, PMT was created based on the expectancy-value theories and the cognitive processing theories. One of the most effective explanatory hypotheses for anticipating a person's inclination to take preventative measures is PMT (Agarwal, 2010). In essence, both the threat and the coping evaluation are the sources of the urge to defend. An individual's judgment of the degree of risk offered by a hazardous occurrence is referred to as a threat appraisal (Rogers R W, 1983) (Mark Chan I. W., 2005). The following two components make it up:

i. Perceived vulnerability is an individual's judgment of the likelihood of dangerous occurrences or threatening events. In this study, threats are a result of ISSP noncompliance.

ii. Perceived severity, or intensity of the event's impact. In this case, failure to comply with the ISSP poses an immediate threat to the security of one's organization's information.

The coping appraisal component of PMT relates to a person's evaluation of their capacity to deal with and prevent any possible loss or damage brought on by the danger (Mark Chan I. W., 2005). Three sub-constituents comprise coping appraisals:

i. Self-efficacy, this factor emphasizes the person's capability or assessment of their capacity to deal with or carry out the advised behavior. This research discusses the abilities and precautions required to protect the information stored in an organization's IS (Jolton, 2005) .

ii. Response efficacy, This factor concerns the person's perception of the advantages of the action they took (John Cacioppo, 1983). Here, it refers to compliance with the ISSP as a reliable method of detecting a threat to one's organizational IS assets.

iii. Response cost, which is a key component, stresses the perceived opportunity costs in terms of money, time, and effort spent on adopting the advised behavior—in this case, adhering to ISSP—in order to comply.

Previous research that employed PMT found that it was useful in anticipating behaviors related to personal computer security behaviors both at home and in organizations (Younghwa Lee K. R., 2009) (Xu, 2009) (Agarwal, 2010) and ISSP compliance (Rao T. H., 2009a) (Mahmood, 2007).

Ajzen developed the Theory of Planned Behavior (TPB) (1991). It makes the claim that attitudes and arbitrary standards have an impact on people's conduct and perceptions of behavioral control. TPB is one of the most effective persuasion theories and has been applied extensively in a variety of fields. The previous body of information has demonstrated that attitude, subjective norms, and perceived behavioral control have a significant impact on a person's desire to comply with ISSP (Venkatesh, 2003) (Burcu Bulgurcu, 2010). The following are descriptions of the three TPB components that were employed in the current study.

i. The definition of attitude is a person's attitude toward engaging in a particular behavior, either positively or negatively. This study, it captures attitudes toward ISSP compliance.

ii. Subjective norms represent a person's understanding of what important people think about a certain behavior.

iii. Perceived behavioral control, the third TPB component was impacted by Bandura's (Bandura A. , 1991)self-efficacy in the social cognitive theory it describes how easy or difficult a person perceives a given activity to be for them to do or facilitate.

TPB has been widely used to examine information system ethics and people's choices to use appropriate computer security measures and adhere to ISSP (Younghwa Lee K. A., 2005); (Kreie, 2004).

3.1 The research model and hypotheses

Following the description above, the research model presented in Fig. 1. It can be seen that both the TPB and PMT are fused as both theories have one common element, self-efficacy, which, as noted above, is the same concept encapsulated by Ajzen (Ajzen, 1991). perceived behavioral control. The behavioral intention of the ISS is the dependent construct. The research hypotheses are discussed after that.

Subjective norms are normative cues, ideas, and desires to perform a certain act that is frequently influenced by discussion or observation of other people's conduct (Ajzen, 1991)

(Aronson, 2010). An individual's conduct has been proven to be impacted or driven by what they perceive to be the norm in their environment (Chan, 2005) (Knapp, 2006) (Johnston Allen, 2010). Employees are more likely to adhere to their organization's ISSP if they observe that those in their immediate surroundings, such as superiors, peers, and subordinates, are following and abiding by such guidelines (Chan, 2005). Subjective norms have a considerable impact on ISSP compliance in businesses, according to research by（Rao T. H., 2009a)（Rao T. H., 2009b)（Burcu Bulgurcu, 2010)（Mahmood, 2007)**.**

3.1.1. Hypothesis 1: Subjective norms will influence ISSP compliance and behavioral intention in a good way.

In the IS literature, there has been extensive testing of the connection between attitude and behavioral intentions (Venkatesh, 2003)**.** According to TPB, people's attitudes affect their behavioral intentions (Ajzen, 1991). In light of this, an optimistic outlook on ISSP compliance portends favorably for ISSP compliance behavioral intention. Negative attitudes, on the other hand, will reduce a person's behavioral intention to comply with the ISSP. People who have good attitudes and beliefs about their organization's ISSP will thus be more likely to adhere to these standards (Angela Sasse and Sacha Brostoff, 2004) (Xu, 2009)**;** (Rao T. H., 2009b)**;** (Burcu Bulgurcu, 2010)**.** However, people who lack such positive attitudes would not readily adhere to such policies (Mahmood, 2007)**;** (Myyry, 2009). It is hypothesized that:

3.1.2. Hypothesis 2: The behavioral intention of ISSP compliance will be positively impacted by attitude toward ISSP compliance.

As previously mentioned, self-efficacy emphasizes a person's abilities and competence to complete a task or make a decision (Bandura, 1977). It has been demonstrated that self-efficacy significantly influences a person's capacity to engage in task behavior, including using IS (Higgins, 1995) (Straud, 2008). According to (Higgins, 1995), those who are more confident in their ability to use information systems in their daily lives would use those systems more frequently than those who are less confident. Regarding ISSPs, it is anticipated that people with high IS security capabilities and competence would understand the necessity of adhering to organizational ISSPs and may be better positioned to recognize the risks of non-compliance. Studies have shown that self-efficacy is relevant to ISSP compliance behavior intention (Burcu Bulgurcu, 2010) (Mahmood, 2007) (Rao T. H., 2009a) (Robert Larose, 2008) (Straud, 2008)**.**

3.1.3. Hypothesis 3: Self-efficacy will influence ISSP compliance behavioral intention in a favorable way.

According to (Mahmood, 2007), reaction costs might include financial outlay, scheduling annoyances, shame, or other unfavorable effects that follow a person's actions. (Straud, 2008) commented that people maintain various cost-benefit perceptions of information security measures that are unrelated to the assets' perceived business value or sensitivity (the gravity of the threat), especially in light of their own self-interest. People are therefore reluctant to follow or adopt suggested answers if they believe that doing so will require investing a significant amount of time, effort, and money (SHEINA, 2000) (Larsen, 2009). On the other hand, a measure may be approved if it just requires a few resources to implement (Cornelia Pechmann and Guangzhi Zhao and Marvin Goldberg, 2003) (Straud, 2008)**.** The likelihood that a person will engage in a recommended behavior tends to rise when the response cost is reduced (Chan, 2005). Response costs are inversely correlated with the inclination to adopt security measures, according to previous studies (Hsu, 2003) (Straud, 2008) (Larsen, 2009).

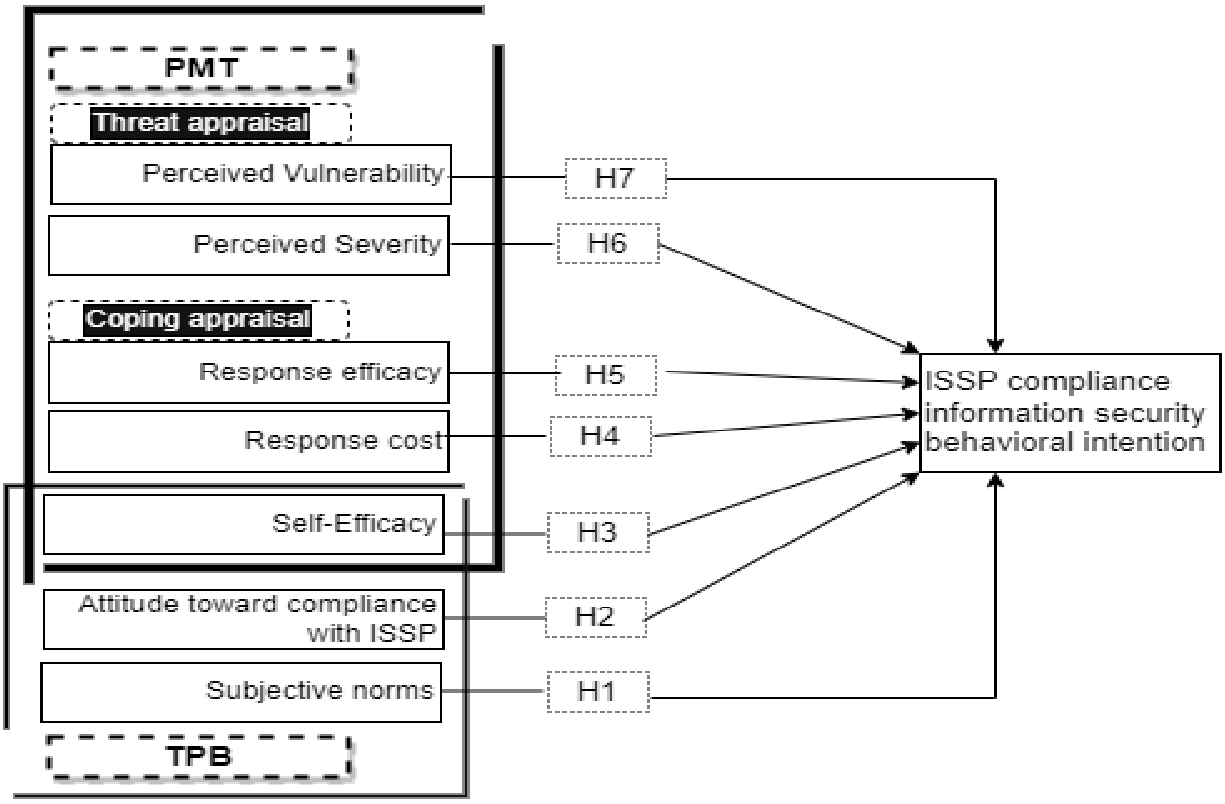


Fig 2: The research model.

3.1.4. **Hypothesis 4:** Response costs will influence ISSP compliance behavioral intention negatively.

An individual is more likely to adopt an adaptive behavior when they have the necessary knowledge about how well a suggested coping strategy works to protect them from a threat or danger (Rogers R W, 1983) (Robert Larose, 2008). On the other side, if the person has less faith in a measure's efficacy, he or she might not embrace it right away (P A Rippetoe, Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat, 1987). As a result, people are more likely to acquire an intention to adopt an ISSP if they think their organization's ISSP contains guidance and coping strategies to avoid hazards and dangers in their setting (Rao T. H., 2009a).

3.1.5. Hypothesis 5: Response efficacy will influence ISSP compliance behavioral intention in a favorable way.

Generally speaking, when people sense danger, they frequently alter their actions in reaction to the risk involved and decide whether or not they are willing to accept the threat (SHEINA, 2000) (Straud, 2008). As a result, an individual's intentions to take preventative measures tend to be positively correlated with their perception of severity (Cornelia Pechmann and Guangzhi Zhao and Marvin Goldberg, 2003). Individual is more likely to adhere to the rules and specifications outlined in their ISSP if they perceive a threat to their organizations IS assets (Burcu Bulgurcu, 2010) (Mahmood, 2007). On the other side, if a person does not feel threatened by using corporate IS resources, he or she could be less worried about following the instructions in their ISSP. According to (Rao T. H., 2009a) study, employees' intentions to implement ISSP are significantly influenced by their perception of the severity of the situation**.**

3.1.6. Hypothesis 6: Perceived severity will have a positive effect on ISSP compliance and behavioral intention.

People who believe they are immune to security dangers are more inclined to disregard security protocols at work when it comes to safe computing within the firm (Rao T. H., 2009a) (Burcu Bulgurcu, 2010) (Mahmood, 2007). On the other hand, it seems sensible to assume that someone who considers their organizations IS resource as being highly vulnerable will be more inclined to engage in defensive activities. Business leaders' intentions to use security solutions in their firms are significantly impacted by their perception of risk, according to research by Lee and Larsen (2009).

3.1.7. Hypothesis 7: Perceived vulnerability will have a positively effect on ISSP compliance and behavioral intention.

4 METHODOLOGY

4.1 Quantitative research

We only know that people have a variety of thoughts. Different researchers and instructors define "quantitative research" in utterly different ways.

Quantitative research is a methodical approach to gathering and evaluating data from a variety of sources, including online questionnaires, polls, and online surveys, as well as from pre-existing data. Quantitative research builds a statistical model to explain what has been seen by measuring numeric value, unaltered data, and detailed convergent data.

Quantitative research is when numerical data are used to learn more about the world in a methodical manner (Burns & Grove cited by Cormack,1991).

Therefore, quantitative research is concerned with quantity, such as the number of values. What are the patterns in the graphics? and evaluate them to make judgments. The goal of the quantitative research approach is to determine the link, within a small sample of individuals, between the experimental variable (Independent variable) and another influence variable (Dependent variable). In quantitative research, results are reached by quantifying those who were really seen.

4.1.1 Benefits of Quantitative Research

- ✓ A lot of information may be gathered using quantitative research methods.
- ✓ Concentrate on a specific study issue to determine the relationship between the independent and dependent variables.
- ✓ The description of statistical models is easy to describe.
- ✓ Reliability is high.
- ✓ Allow identifying the unrealized relationship among the investigated variable.

4.1.2 How to work Quantitative Research:

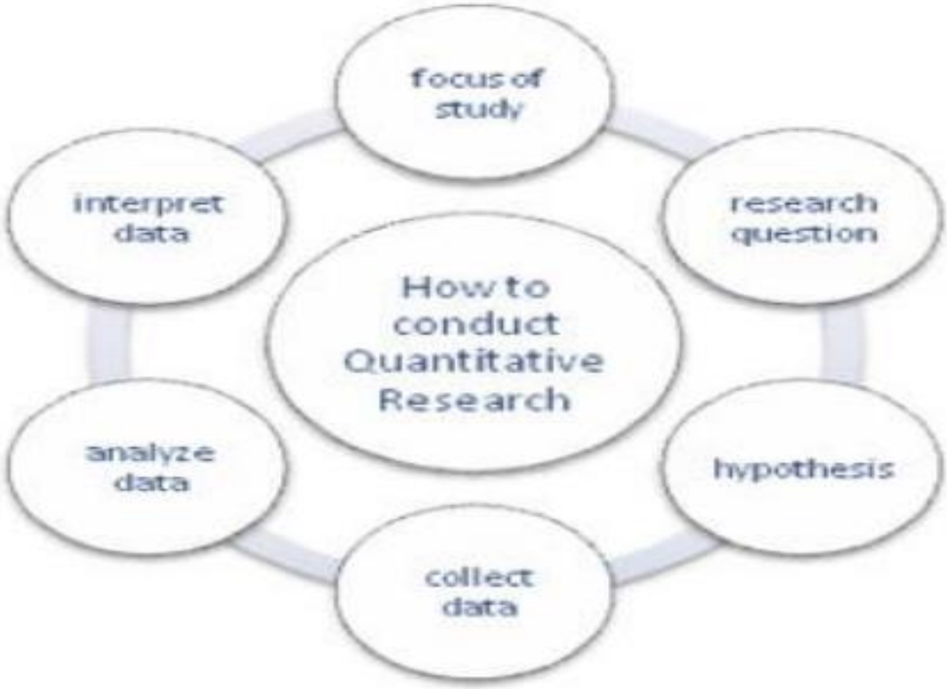


Figure 3: Research process stage

4.1.3 Why we use quantitative research

There are three primary categories of research design methodologies: qualitative, quantitative, and hybrid methods. This collection of modules is centered on quantitative research.

This allows us to categorize characteristics, count them, and build a statistical model. A survey paper makes it simple to ask specialized, focused questions, gather information from respondents, and make an effort to explain what was seen.

In a nutshell, social life is the subject of quantitative study. In quantitative research, when things are assessed, a smaller sample raises the concern that the research's entire population would be affected (Harry & Lipsky, 2014) (Thompson, 2011). In order to predict, confirm, control, and test hypotheses in those many items, this quantitative study collects data that amounts to something. Although quantitative approaches offer benefits, they also have very few drawbacks. This indicates that certain hypotheses provide good results while others produce negative results when quantitative tools are used to build new theoretical thinking. Our research method tries to find the answer to the questions starting with how many, how much, and to what extent(Rasinger 2013).

4.2 Sample Size

Before research is done, proper analyses offer a useful means of regulating statistical power (Hager,2006, Faul et al. 2007). The estimated sample size was determined based on the endogenous variable using the program G*power. Our sample size requirement for this study was 153.

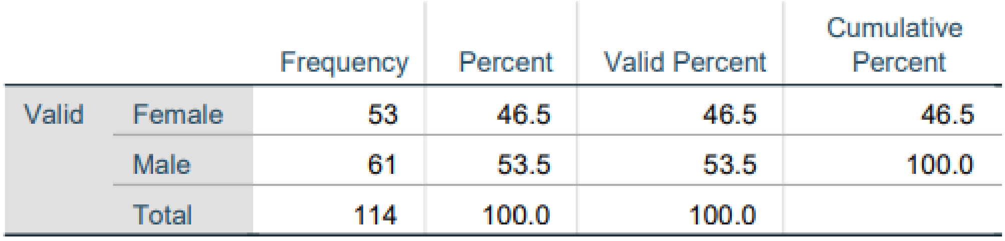
4.3 Data collection procedure

The research model was tested using a survey. To that end, we used two methods to collect our data. For this study, employees of various companies were asked through Google Forms. And distributed the question paper (hard copy) among the students of Daffodil International University. Each participant received a cover letter, questionnaire and a self-address. To improve ISSPs' understanding of organizations, IS experts' viewpoints were also sampled (Rao T. H., 2009a) (Larsen, 2009) (Burcu Bulgurcu, 2010). Since we could not compile a list of IS professionals in Bangladesh, we distributed Google forms to Daffodil International University students and various organizations' staff members. Then, we received 114 answers in all. The sample size required for the study model to be significant, according to a power analysis calculator, was 153. There were two sections to the questionnaire. The first component included demographic data, and the second piece concentrated on elements to gauge the model's building blocks.

4.4 Demographic Information

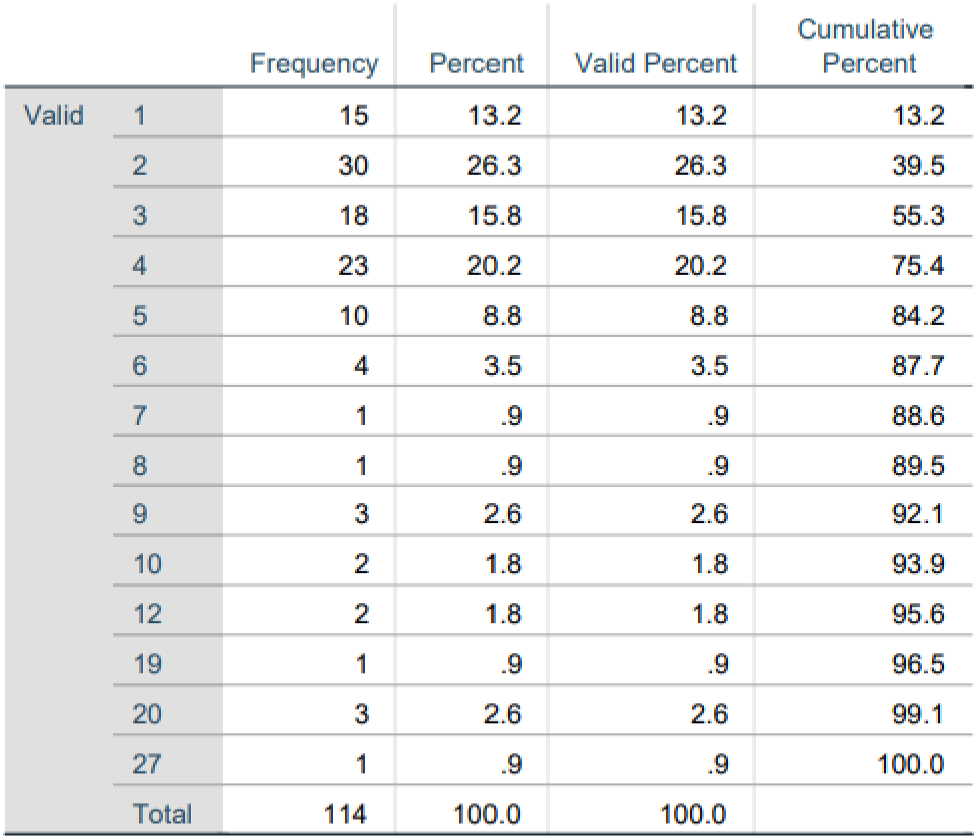
Demographic Data Characteristics of the population. Common examples of population characteristics used in surveys include gender, age, number of years working in the organization, education level, occupation, current position, industry, monthly salary (BDT) usage, etc.

Out of about 114 particular persons, most of them were 20-30 years which a percentage was 88.6%; below 20 years i.e., 11, to 20 years, were 2.6% and 31-40 were nine, i.e. 7.9%, and there one person above 40 years, i.e., .9%, In terms of gender, out of 114, 53.51% are males, and 53 of which are 46.5% of females. And here, we saw that the number of employees with 1 to 10 years of work experience working in the organization was 92.28%, and the number of employees with 11 to 27 years of experience was 8.71%. Among the workers, 28.9% had bachelor's degrees, 13.2% had master's degrees, 4.4% had a Ph.D. degree, 20.2% were diploma holders, and 33.33% had secondary and other. Employees were asked about their position in their workplace. Out of 114 responses, 21 were junior staff, 68 were the most mid-level personnel, and 25 were top management personnel. And these employees were working in different organizations. The number of employees in educational institutions was 16.7%, the number of employees working in finance and insurance companies was also 16.7%, the percentage of employees working in government, healthcare, manufacturing, wholesale, and IT organizations was 19.3% respectively 13.2%, 7.9%, .9%, 10.45%, 14.9%. All of the employees have real-world experience. Tables 1 through 7 would display all information.



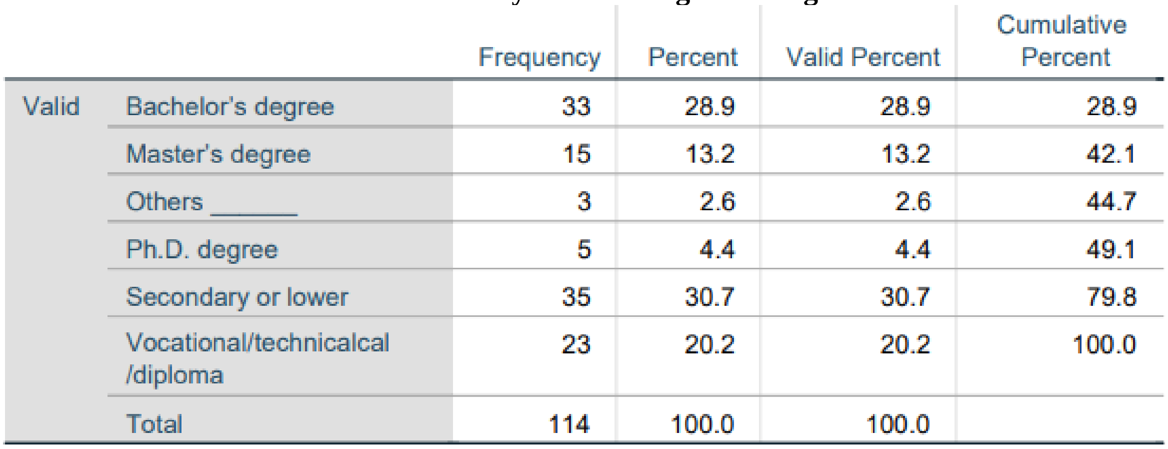
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	53	46.5	46.5	46.5
	Male	61	53.5	53.5	100.0
	Total	114	100.0	100.0	

Table 1: Gender



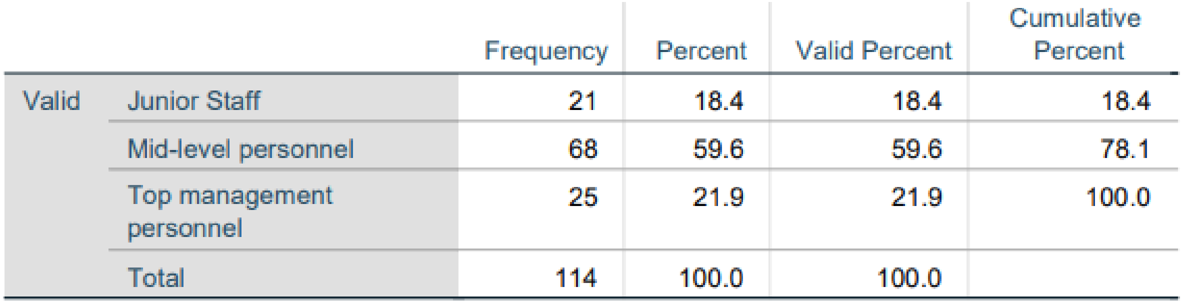
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	15	13.2	13.2	13.2
	2	30	26.3	26.3	39.5
	3	18	15.8	15.8	55.3
	4	23	20.2	20.2	75.4
	5	10	8.8	8.8	84.2
	6	4	3.5	3.5	87.7
	7	1	.9	.9	88.6
	8	1	.9	.9	89.5
	9	3	2.6	2.6	92.1
	10	2	1.8	1.8	93.9
	12	2	1.8	1.8	95.6
	19	1	.9	.9	96.5
	20	3	2.6	2.6	99.1
	27	1	.9	.9	100.0
	Total	114	100.0	100.0	

Table 2: Number of years working in the organization



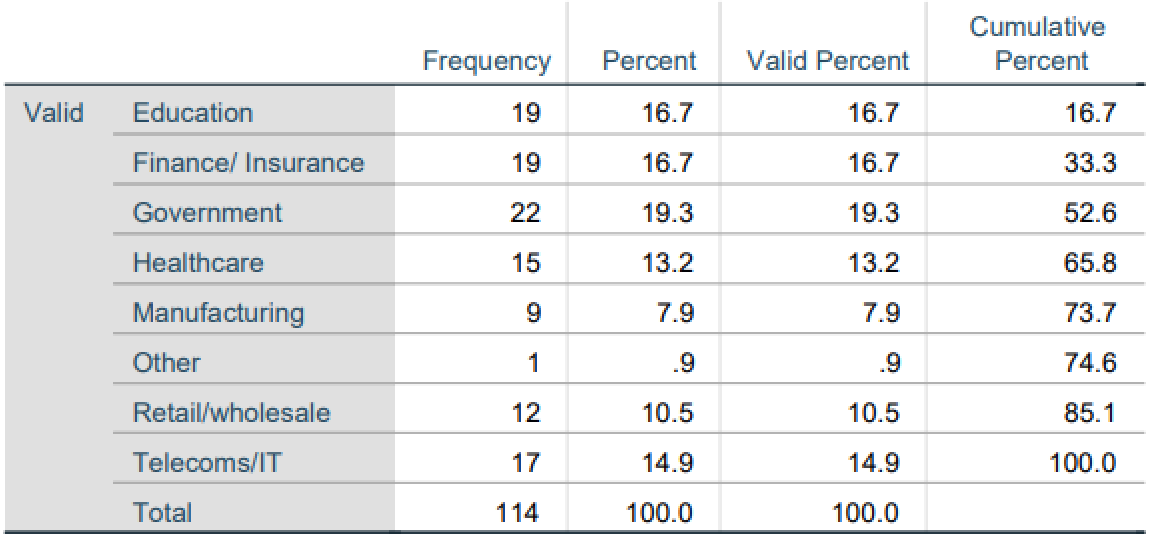
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Bachelor's degree	33	28.9	28.9	28.9
	Master's degree	15	13.2	13.2	42.1
	Others _______	3	2.6	2.6	44.7
	Ph.D. degree	5	4.4	4.4	49.1
	Secondary or lower	35	30.7	30.7	79.8
	Vocational/technicalcal /diploma	23	20.2	20.2	100.0
	Total	114	100.0	100.0	

Table 3: Level of education



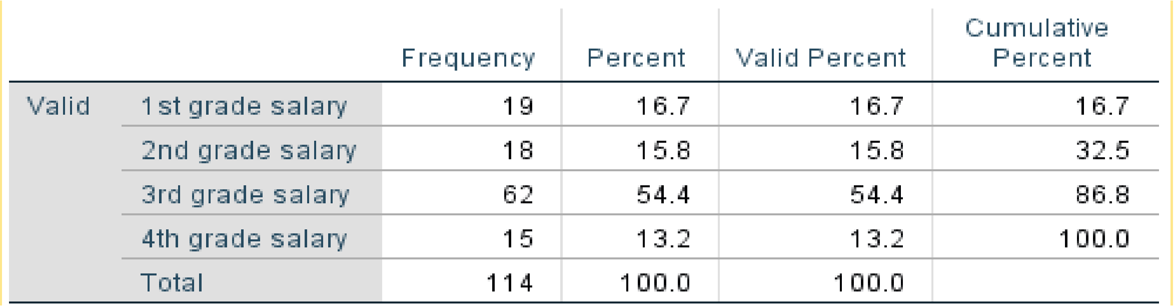
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Junior Staff	21	18.4	18.4	18.4
	Mid-level personnel	68	59.6	59.6	78.1
	Top management personnel	25	21.9	21.9	100.0
	Total	114	100.0	100.0	

Table 4: Current position



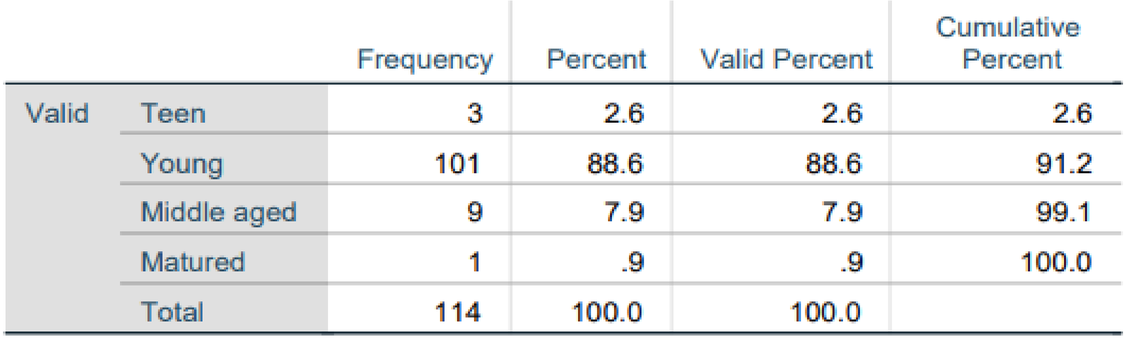
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Education	19	16.7	16.7	16.7
	Finance/ Insurance	19	16.7	16.7	33.3
	Government	22	19.3	19.3	52.6
	Healthcare	15	13.2	13.2	65.8
	Manufacturing	9	7.9	7.9	73.7
	Other	1	.9	.9	74.6
	Retail/wholesale	12	10.5	10.5	85.1
	Telecoms/IT	17	14.9	14.9	100.0
	Total	114	100.0	100.0	

Table 5: Industry



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1st grade salary	19	16.7	16.7	16.7
	2nd grade salary	18	15.8	15.8	32.5
	3rd grade salary	62	54.4	54.4	86.8
	4th grade salary	15	13.2	13.2	100.0
	Total	114	100.0	100.0	

Table 6: Monthly salary of employee



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Teen	3	2.6	2.6	2.6
	Young	101	88.6	88.6	91.2
	Middle aged	9	7.9	7.9	99.1
	Matured	1	.9	.9	100.0
	Total	114	100.0	100.0	

Table 7: Age Group

4.5 Data analysis technique

To analyze our survey variables to build a model or develop a theory, we used SPSS and Smartpls4, and ANN software.

Launched in 1968, the program's initial name was Statistical Package for the Social Sciences (SPSS). One of the most widely used statistical programs is SPSS, which can manipulate and analyze detailed data with only a few basic instructions. SPSS provides the capacity to handle string data. With SPSS, we discover:

- Easily and quickly displays data tables
- Easily add missing data
- It gives bar chart and demographic table

PLS and the ANN approach are two-stage analytical methodologies for testing and validating the suggested model. This study will first formulate a few hypotheses. It was then used a box and arrow to depict the relationships. Then, using additional analysis, it will determine whether or not those associations are significant. PLS allows for testing of the proposed linkages. ANN modeling will be utilized in the second stage to validate the PLS outcome. This will establish the importance of each significant association so that the study can quickly identify the most crucial element influencing the ISSP compliance behavioral intention. Because it outperforms conventional methods in identifying linear and non-linear interactions rather than simply linear ones, ANN will be used in this investigation.

5 DATA ANALYSIS AND RESULTS

5.1 Measurement model

Researchers "must test the outer model once the research model was established," according to (Kurnia, 2017).

To put it simply, a measurement model is the component of a model that investigates the relationships between hidden variables and connects measurable variables. Reflective indicators are used to measure each pickup variable within the study model that is currently being presented. The following two criteria—constructive validity and discriminative validity—must be used to validate the measurement model.

5.2 Reliability and validity analysis

Three stages of statistical data analysis were completed. In the first phase, the conceived research model's validity was evaluated. Cronbach's alpha coefficient value was taken into consideration while assessing the dependability of model variables. Confirmative factor analysis was also used to examine the composite reliability, convergent and discriminant validity, and reliability. In the second phase of the study, hypotheses were tested using maximum likelihood estimation and partial least squares (PLS). The third phase was confirming, with the use of neural networks, the degree of the influence that independent factors had on dependent variables, the relevance of which had been shown through PLS analysis. The Statistical Package for Social Sciences (SPSS) and SmartPls were used for data analysis.

5.2.1 Construct reliability

Composite reliability (CR) (Larcker, 981), which should be 0.7 or higher (Hair et al. 2014), and average variance extracted (AVE), which should be 0.5 or higher, define the quality at the extract level. According to AVE, properly convergent LVs should have measures with less than 50% error variance and more than 50% explained or common variance in the factor analytic sense. For additional information, see Dillon and Goldstein (1984). Concerning X, their Average Variance Extracted (AVE) signs x1, x2,... x^n are:

$$\frac{(\ )}{[\ ]\ (\ ) + [\ (\ )]}$$

Where λi is the loading of xi on X, Var denotes variance, is the measurement error of xi, and Σ denotes a sum (Fornell & Larker, 1981). To get better AVE, we removed some questionnaire data. Both criteria are fulfilled, as shown in Tables 9 and 10.

	Average variance extracted (AVE)
ATI	0.514
ICB	0.533
PS	0.587
PV	0.552
RC	0.591
RE	0.528
SE	0.587
SN	0.606

Table 8: AVE

	Composite reliability (rho_c)
ATI	0.805
ICB	0.819
PS	0.809
PV	0.831
RC	0.811
RE	0.769
SE	0.809
SN	0.822

Table 9: Composite reliability

5.2.2 Discriminate Validity

When the extent of measurement item differences between one another is described by discriminate validity (Campell and Fiske, 1959).. For this reason, the square root of AVE is shown in Table 10's hidden variable correlation diagonal. It can be said that our measurement model is valid because these values are higher than the corresponding construct correlation.

	ATI	ICB	PS	PV	RC	RE	SE	SN
ATI	0.717							
ICB	0.453	0.73						
PS	0.58	0.638	0.766					
PV	0.477	0.574	0.472	0.743				
RC	0.357	0.452	0.546	0.294	0.768			
RE	0.404	0.415	0.342	0.498	0.193	0.727		
SE	0.56	0.466	0.525	0.443	0.31	0.475	0.766	
SN	0.283	0.603	0.512	0.631	0.359	0.371	0.391	0.779

Table 10: Discriminate Validity

5.2.3 F^2

F2 measures are used to determine the impact of the independent variable. (Cohen, 1988)Cohen (1988) specifies the thresholds of 0.02, 0.15, and 0.35 as measuring small, medium, and large effects. Table 11 shows the F^2 result.

	ICB	Effect Size
ATI	0.001	Small
PS	0.93	large
PV	0.03	Small
RC	0.018	Small
RE	0.15	Medium
SE	0.003	Small
SN	0.07	Small

Table 11: F^2 effect size

5.2.4 Structural model

In a nutshell, the relationship between the hidden variables is the structural model. A theoretical model's structural model reveals causal and correlative relationships between its hidden variables.

5.2.5 Coefficient of determination (R^2)

The coefficient of determination (R^2) and significance levels of each path coefficient is used to evaluate the structural model (Chin, 1998). Table 12 shows the R2 result.

	R-square	R-square adjusted
ICB	0.557	0.527

Table 12: Coefficient of determination

5.2.6 Hypotheses test

The suggested model's links between the hypotheses were examined using the structural equation model. The intensity and significance of the direct effects of seven independent factors on ISSP compliance behavioral intention were assessed for the seven relations that were specifically evaluated. Two associations out of a total of seven that were examined were statistically significant (Table 13). Only usefulness, out of the two usability-related criteria (usefulness and simplicity of use), significantly influences ISSP compliance behavioral intention ($p < 0.05$). As a result, both hypotheses H1 and H6 are supported. However, because there was no statistically significant relationship between the ease of use and behavioral intention in the model ($p > 0.05$), hypotheses H2, H3, H4, H5, and H7 are all discarded. Seven hypotheses were formulated based on the relevant literature, and the data suggested that two were highly significant. The attitude towards compliance, self-efficacy, response cost, response efficacy, and perceived vulnerability ($\beta = 0.313$, $p < 0.755$), ($\beta = 0.598$, $p < 0.55$), ($\beta = 1.199$, $p < 0.231$), ($\beta = 0.929$, $p < 0.353$), ($\beta = 1.531$, $p < 0.126$) were significantly negative and subjective norms ($\beta = 2.836$, $p < 0.005$), perceived severity ($\beta = 2.828$, $p < 0.005$) effect on the information security behavioral intention. So we can say that H1 and H6 are significantly supported, but H2, H3, H4, H5, and H7 are not supported because there is a lack of knowledge about information system security policy behavioral objectives in Bangladeshi organizations.

Number	Hypothesized Path	Original sample (O)	T statistics (|O/STDEV|)	P values	Result
H1	**SN -> ICB**	0.247	2.836	0.005	Supported
H2	**ATI -> ICB**	0.029	0.313	0.755	Not supported
H3	**SE -> ICB**	0.047	0.598	0.55	Not supported
H4	**RC -> ICB**	0.108	1.199	0.231	Not supported
H5	**RE -> ICB**	0.081	0.929	0.353	Not supported
H6	**PS -> ICB**	0.304	2.828	0.005	Supported
H7	**PV -> ICB**	0.167	1.531	0.126	Not supported

Table 13: Hypothesis testing result

5.2.7 Hypothesis test diagram

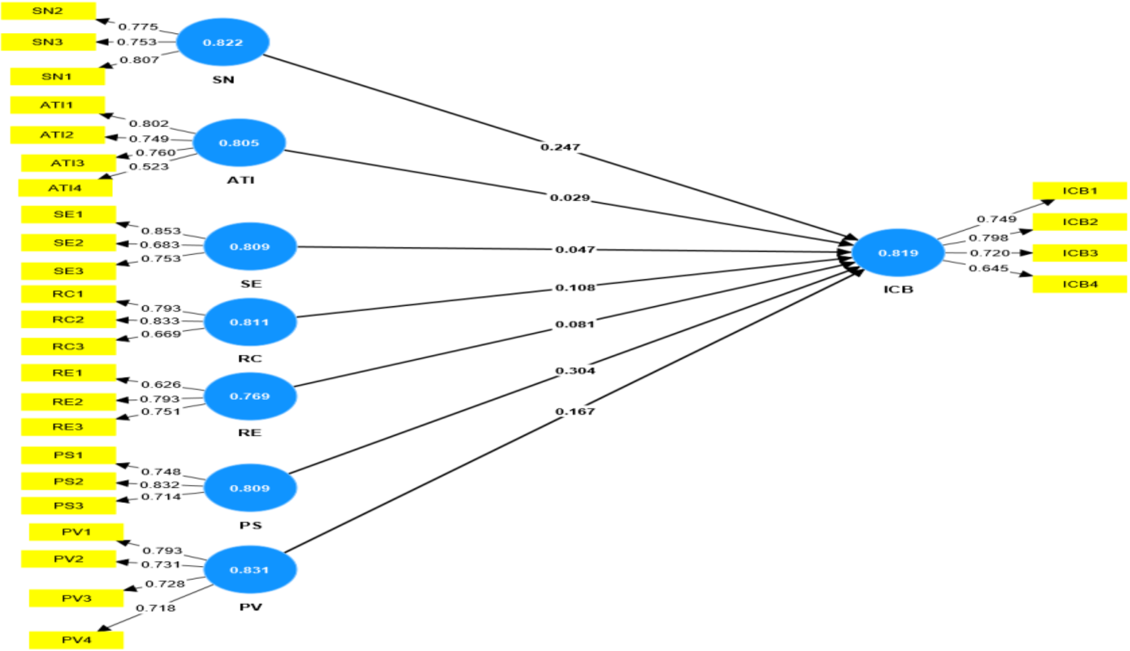


Figure 4: The SmartPLS 4.0 results for the tested hypotheses.

5.3 Artificial Neural network analysis

By integrating SEM with neural network analysis, one of the most effective artificial intelligence approaches, this study uses a multi-analytical strategy. Traditional linear statistical methods, such as PLS, SEM, and Multiple Regression Analysis (MRA), may only identify linear associations, which may cause complicated decision-making processes to be oversimplified (Chong, 2012). The use of an artificial neural network model, which can spot non-linear correlations, is advised as a solution to this issue. This method allows the neural network model to learn intricate linear and non-linear relationships between predictors and the adoption decision (Chong, 2012). A massively parallel distributed processor made up of basic processing units with a neural tendency for storing experimental information and making it accessible to users is an artificial neural network (ANN), according to (Haykin, 2001). The biological neurons in the brain are comparable to these basic processing units, often known as neurons or nodes. ANN acquires knowledge through the process of learning, and it is then stored in interneuron connection strengths known as synaptic weights (SPSS 26).

There is no specific formula for choosing the ideal number of hidden neurons, despite its significance. It should be highlighted that, in some circumstances, all these generalizations should be tested before being used in full. In most circumstances, choosing the network that performs best on the testing set with the fewest hidden neurons is desirable. Numerous additional elements, such as the number of hidden layers, sample size, neural network design, complexity of the activation function, training technique, and others, may also have an impact on the decision about the number of hidden neurons (Sheela K. G., 2013).

Trust, perceived utility, personalization, and customer participation are the seven significant PLS variables that make up our research's input layer of the neural network. One output variable makes up the output layer (ISSP behavioral intention). The number of nodes in a single hidden layer is fixed to two in accordance with the aforementioned suggestions. Neurons in the hidden and output layers are activated using the sigmoid functions (Chong, 2012) (Ooi, Predicting the determinants of the NFC-enabled mobile credit card acceptance: A neural networks approach, 2013). All inputs and outputs were standardized to the range [0,1] in order to improve training efficacy, i.e., to allow for shorter training times and greater performance (Negnevitsky, 2005).

Ten-fold cross-validation was used to prevent over-fitting, with 70% of the data used for network training and the remaining 30% for testing or evaluating the trained network's predictive accuracy (Sheela K. G., 2013) (Alain Chong, 2015).

The Root Mean Square of Error (RMSE) of the training and testing data sets for each of the ten neural networks and the averages and standard deviations for both data sets are calculated and provided in Table 14 as a measure of the predictive accuracy of the model.

The neural network model's average RMSE is relatively low (20.21 for training data and 7.38 for testing data), indicating a reasonably accurate forecast (Ooi, Predicting the determinants of the NFC-enabled mobile credit card acceptance: A neural networks approach, 2013) (Hew, 2014).

The significance of each independent variable is a measure of how much the value predicted by the network model changes depending on the independent variable's value (Chong, 2013a). The normalized importance is the ratio of each predictor's relevance to its maximum value. Table 15 displays the sensitivity analysis's findings.

Neural Network	Training Data	Testing Data
ANN1	19.58	5.25
ANN2	21.48	10.00
ANN3	20.72	4.71
ANN4	15.96	11.73
ANN5	19.89	6.28
ANN6	21.46	7.85
ANN7	20.89	5.95
ANN8	19.68	7.13
ANN9	25.49	5.23
ANN10	16.94	9.65
Average	20.21	7.38
Standard deviation	2.61	2.38

Table 14: RMSE values for the neural networks.

Predictors	Normalized Importance
Perceived Severity	93.5%
Subjective Norms	91.7%

Table 15: Normalized variable importance.

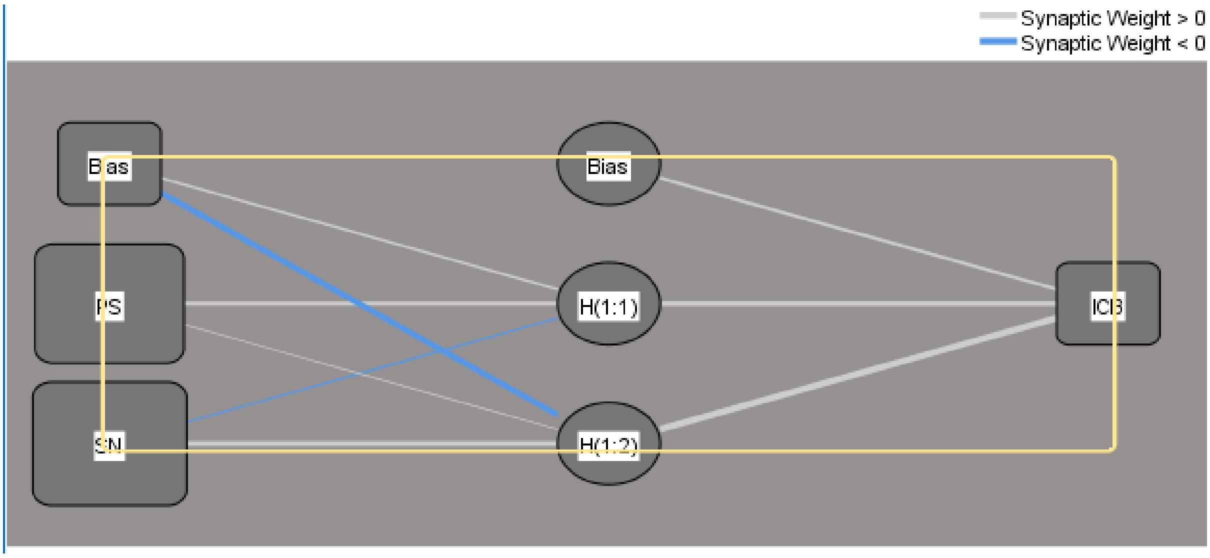


Figure 5: Network diagram

Customization, followed by consumer engagement, trust, and utility, is the most crucial predictor of ISSP compliance behavioral intention acceptability, according to the provided neural network research.

6 DISCUSSION

This research created and verified a model to further our knowledge of ISSP compliance in businesses by merging two pertinent theories: PMT and TPB. The study's findings demonstrate that the model's independent variables successfully predicted a sizeable portion of the variation in the dependent variable—ISSP compliance behavioral intention—of the proposed model.

It was discovered that the two TPB components, subjective norms and attitude toward compliance, significantly improved ISSP compliance behavioral intention. These findings suggest that ISSP behavioral intentions are strongly influenced by employees' perceptions of ISSP compliance in their firms and colleagues' perspectives. Employees are more likely to adopt their organization's ISSP if they have the necessary competence and capability to implement preventative security measures, according to the result related to the third component of TPB, i.e., self-efficacy, which is also present as one completes the coping appraisals in PMT.

The research is exceptionally distinctive since it uses a cutting-edge technique combining partial least squares (PLS) with artificial neural networks (ANN). In this way, neural networks were also employed in the research, allowing for further validation of the PLS analysis's output after validating the model and examining the impact of independent factors on the dependent variable. The work offers management implications for ISSP compliance behavioral objectives as well as functional theoretical consequences for academic researchers and academics.

6.1 Theoretical implications for research

Researcher implications are provided by this study. A research conceptualization that blends PMT and TPB in the context of people's or workers' ISSP behavioral intention is first proposed and validated in this study. To that aim, this research suggests that combining the two theoretical frameworks improves knowledge of the variables influencing employees' ISSP behavioral compliance compared to using each theoretical framework independently to examine the issue. Second, because such an approach increases our understanding of the field, researchers looking into ISSP behavioral compliance in businesses should think about merging theoretical viewpoints from many areas.

Second, this study supports TPB and PMT by showing that elements including self-efficacy, response efficacy, social norms, compliance attitude, and perceived vulnerability have a beneficial impact on employees' ISSP behavioral compliance. Our findings demonstrate that societal imperatives, individual attitudes, threats, and coping assessments constrain ISSP compliance behavioral intention, which is consistent with the postulates of the theories used in this study. Fourth, this study expands information about IS security practices in businesses from the perspectives of both cohorts by taking into account the viewpoints of both IS professionals and non-IS managers. Such things must be taken into account to improve understanding (Lee and Kozar, 2005; Herath and Rao, 2009a). Fifth, this study adds to the body of research that has demonstrated that variables including self-efficacy, response efficacy, social norms, compliance attitude, and perceived vulnerability do affect employees' behavioral compliance with ISSP. Sixth, this research, together with related initiatives in the field, presents a chance for the creation of a thorough, integrated contingency model for evaluating ISSP compliance in businesses.

6.2 Limitations and directions for future research

Certain shortcomings in the current research give fresh possibilities for further investigations. First, in an effort to uphold their company's reputation, some IT experts may have provided answers to some socially acceptable inquiries (Philip M Podsakoff, 2003). As a result, it's possible that the responses were altered to harm the data analysis. The present research's first possible restriction is that we only included a small number of organizations and a few university students in our study who were somehow involved in policy compliance is the first possible drawback of the current research. This work should be applied to different socio-cultural environments for future investigation. Except for hypotheses 1 and 6, all other hypotheses lack support. Better assessments of this notion will be developed in subsequent investigations. This study should be repeated in the future with larger samples drawn from other industries. In the current study, a two-stage analytical approach (PLS-ANN) was employed for the validation of the research model. Other nonlinear techniques, such as support vector machines, fuzzy sets, and random forests, which are utilized for reliable predictive analysis, also need more research before they can be put to use. Future studies might examine actual information security protective behaviors and deepen insights by using qualitative research techniques like focus groups and in-depth interviews.

Second, the study's focus was on IS experts working for Bangladeshi companies. If the cultural values of the relevant groups had an influence on the results, then the results' generalizability could have been compromised. Third, this study focused on the opinions of IS personnel regarding information security protective measures. In order to advance knowledge in this area, future research may examine the perspectives of workers not directly involved in information security, such as those of outsourced labor. This would make it possible to compare people's behavior at work under various levels of information security regulation, raising awareness of the issue.

Future research might analyze the viewpoints of contractors and other personnel that firms use in this era of outsourcing to further our understanding in the field. The current study concentrated on workers' perceptions of ISSP compliance. To further our understanding of the topic, comparative examination of employees' ISSP behavioral compliance habits in nations with high and low privacy rules might be looked at. The external elements that influence employees' and other staff members' compliance with the ISSP should be discussed, as well as any potential effects they may have on the rational behaviors of employees in relation to the effectiveness and costs of their responses. There hasn't been much study on how to communicate ISSP in a way that doesn't foster or build fear, uncertainty, or despair (FUD) in staff members.

7 CONCLUSION

Organizations' attempts to safeguard their IS assets served as the inspiration for the current study. To succeed on these fronts, organizations occasionally purchase technical instruments. Organizations occasionally concentrate on implementing ISSP in their environments. If employees don't follow the rules and standards, what use are the policies and guidelines? This study used TPB and PMT, two pertinent behavioral intention and persuasive theories, to further understand the field. The opinions of corporate managers and IT specialists were surveyed. The results of the study demonstrated that perceived severity and subjective norms positively influence ISSP behavioral compliance intention. This study project improves our understanding of ISSP behavioral patterns of employees. This study project improves our comprehension of employees' ISSP behavioral patterns.

8 SURVEY QUESTIONNAIRE

Item	Description	Source
Subjective Norms		
SN1	My manager thinks I should follow the Information System Security Policy of the company (ISSP).	(Ifinedo, 2012)
SN2	My coworkers considered that I should protect the security of the organization's information assets by following the ISSP.	
SN3	The IT department of my company puts pressure on me to follow the company's ISSP and protect the security of information assets.	
SN4	The subordinates who work under me think that I must follow the organization's ISSP.	
Attitude		
ATI1	It is smart to follow the ISSP of the organization.	(Herawan, 2015)
ATI2	Information security best practices for users are helpful, and users must follow the company's ISSP.	
ATI3	It is important to follow the organization's ISSP.	
ATI4	I think that users' actions to protect their data are important for protecting their data.	
Self-efficacy		
SE1	I know how to defend myself against information security infractions because I have the right skills.	(Straud, 2008)
SE2	I know how to stop people from getting my private information by putting in place preventive measures.	
SE3	I know how to stop people from hurting my work computer by putting in place safety measures.	
SE4	I think I have the power to keep myself safe from information security breaches.	
SE5	I can set up security measures on my work computer, but I can't do it without manuals.	
Response cost		
RC1	Putting in place IS security measures cost my company too much in overhead costs.	(Straud, 2008)

RC2	Setting up IS security measures in my company would take a lot of time.	
RC3	The difficulty of implementing IS security policy recommendations outweighs the potential benefits.	
RC4	Other than time, using information security measures would require a significant investment of effort.	
RC5	The disadvantages of the suggested security measures outweigh the benefits for my company.	
Response efficacy		
RE1	By turning on the security features on my work computer, I can stop hackers from getting in.	(Ifinedo, 2012)
RE2	By turning on security measures at my workplace, hackers won't be able to get to important financial or personal information.	
RE3	At my job, steps are taken to keep my confidential information safe.	
RE4	The measures available to protect my company's information from security breaches work well.	
Perceived severity		
PS1	I think that keeping my organization's information safe is important.	(Straud, 2008)
PS2	Having someone hack into and damage my computer at work is a big deal.	
PS3	My organization's data security is at risk of not following the information system security policy (ISSP).	
PS4	I take an attack on my company's IS security very seriously.	
PS5	My computer's and my data's vulnerability in terms of security concerns at work is Network Vulnerabilities, Process Vulnerabilities, and OS Vulnerabilities. Human Vulnerabilities.	
PS6	At work, it's a big problem for me if someone looks at my private information without my permission or knowledge.	
PS7	Hacking is a big problem for me because it can cause me to lose data.	
Perceived vulnerability		
PV1	If I don't follow my companies IS policy, there could be security holes in my company.	(Ifinedo, 2012)
PV2	If I don't follow the IS policy of my company, I could be the target of an attack.	

PV3	Trying to keep my company's information safe will make it harder for illegal access to get to it.	
PV4	If I follow the rules, the information and resources of my organization may be safe.	
PV5	The chances of an information security breach happening at my job.	
PV6	The chances of harming my organization’s computer and information systems.	
PV7	Security breaches could happen to the information and data of my organization.	
ISSP compliance behavioral intention		
ICB1	I want to keep up my adherence to the organization's ISSP.	(Ifinedo, 2012)
ICB2	I'm confident I'll follow the ISSP for my organization.	
ICB3	It is conceivable that I will adhere to the organization's ISSP in order to safeguard its information systems.	
ICB4	I want to continue adhering to the organization's ISSP in the future.	
ICB5	Whenever feasible, I would adhere to the company's security policy.	

Table 16: The measurements, items and their descriptive statistics.

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

AkmarIsmail, 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

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

Bhaharin, 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

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. (981). 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

Myyry, 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

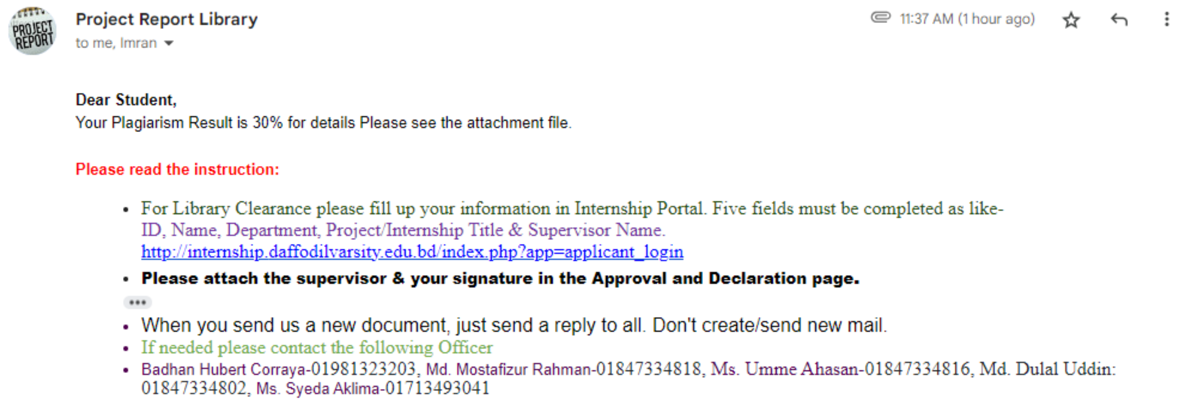
Xu, B.-Y. N. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*, 815-825. doi:https://doi.org/10.1016/j.dss.2008.11.010

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



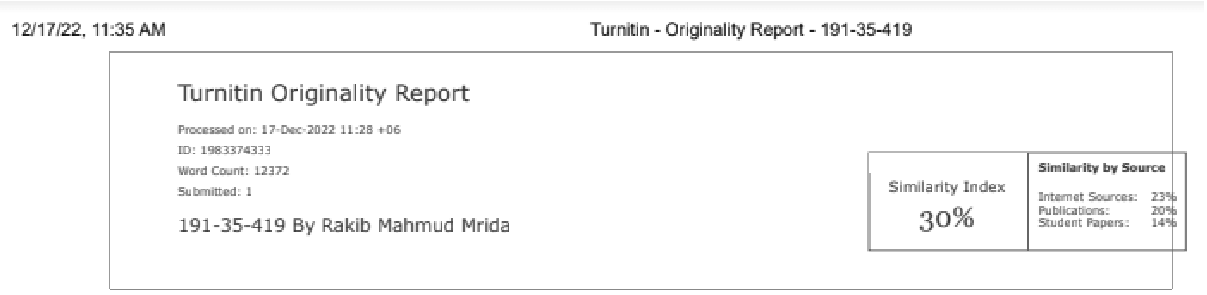
Project Report Library
to me, Imran

11:37 AM (1 hour ago)

Dear Student,
Your Plagiarism Result is 30% for details Please see the attachment file.

Please read the instruction:

- 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
- **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



12/17/22, 11:35 AM Turnitin - Originality Report - 191-35-419

Turnitin Originality Report

Processed on: 17-Dec-2022 11:28 +06
ID: 1983374333
Word Count: 12372
Submitted: 1

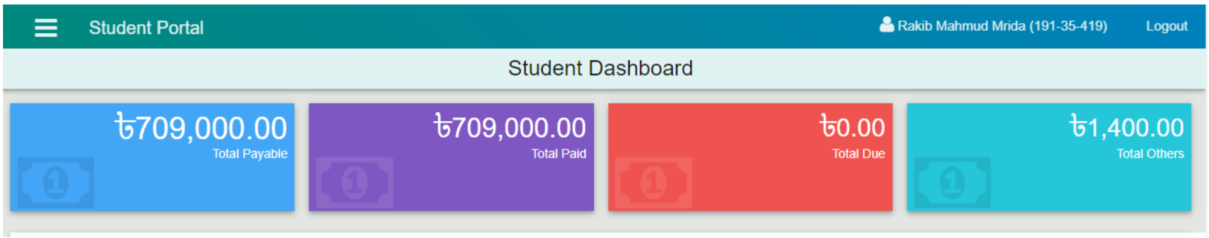
191-35-419 By Rakib Mahmud Mrida

Similarity Index
30%

Similarity by Source

Internet Sources:	23%
Publications:	20%
Student Papers:	14%

ACCOUNT CLEARANCE



Student Portal

Rakib Mahmud Mrida (191-35-419) Logout

Student Dashboard

৳709,000.00	৳709,000.00	৳0.00	৳1,400.00
Total Payable	Total Paid	Total Due	Total Others