**Developing Awareness to Basic Fundamentals about Information Security Management for BSAIS students of CARD-MRI Development Institute**

A Research Paper

Presented to the Faculty of the

CARD MRI Development Institute Inc.

Bay Campus

Bay, Laguna

In Partial Fulfillment

Of the Requirement for the Degree of

Bachelor of Science in Accountancy

Acuña, Meriam

Alamag, Raphael P.

Alias, Cyrus kylle L.

Bañadera, Zyra B

Bathan, Richard Daniel L.

Conchada, Ma. Hannah V.

Damiles, Joan O.

2022

**Abstract:**

Information security refers to protecting your information and data from cyber-attacks such as hacker attacks, phishing scams, and third parties. Throughout this study, they will address the developing stage of the students at CMDI as they represent the advantages of information security profoundly and identify the potential threats that lay beneath this topic. Information security is the process of preventing hackers from accessing data information. Hence, learning its fundamentals as quickly as possible to minimize any unsafe situations when executing those skills and knowledge through employment and simulation software is essential, particularly for students pursuing a Bachelor of Science in Accountancy Information System.

Keywords:

Information Security, Cyber-Attacks, Risk and Threats, Development, fundamentals

**TABLE OF CONTENTS**

**CHAPTER 1 THE PROBLEM AND ITS BACKGROUND**

Introduction

Structure and Rationale of the Study

Statement of the Problem

Objectives of the Study

Significance of the Study

Limitations of the Study

Definition of Terms

**CHAPTER 2 REVIEWS OF RELATED LITERATURE AND STUDY**

Related Literature

Related Studies

**CHAPTER 3 RESEARCH METHODOLOGY**

Research Design

Research Procedure

Research Instrument

Statistical Treatment

**CHAPTER 4 PRESENTATION, ANALYSIS, AND INTERPRETATION OF DATA**

**CHAPTER 5 SUMMARY, FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS**

Summary

Findings

Conclusions

Recommendations

BIBLIOGRAPHY

APPENDICES

Appendix A

Appendix B

**CHAPTER I**

**THE PROBLEM AND ITS BACKGROUND**

Introductory Statement

Information securities are the processes and methodologies widely used for a different business transactions, educational systems, and financial activities that protect their important data for cyber-attacks. The advancement of the Cyberworld in this time may give people convenience and risk. According to Ludwig Slusky & Parviz Partow-Navid (2014 As cyber threats continue to proliferate at an exponential rate, the need for information security awareness training extends far beyond the scope of the Information Technology college curriculum. Information security spreads into new areas of knowledge and becomes more contextually aware. As a result, information awareness training at the college level must be tailored to students' practices more specifically. This paper presents the findings of an information security survey conducted in the spring of 2011 among students in the College of Business and Economics at California State University, Los Angeles.

Several character traits of students' practices and their awareness of risks and protection mechanisms related to computer skills, mobile computing, data loss and encryption, online social networking, awareness training, a correlation between practice and awareness, and others were revealed by the survey.

According to the survey, the main issue with security awareness is not a lack of security knowledge but rather how college students apply that knowledge in real-world situations. Simply put, complying with information security awareness is lower than comprehension. The findings described in this study intended to help colleges design a curriculum that provides as much situationally Data Protection training.

Information Security is an important contributing factor for success in having a security plan and should be properly assessed to comprehend improvements. Information security is generally lacking in planning and managing as they are exposed to much data that can interest hackers and scammers. Since it usually consists of utilizing information security terms to lessen security risk.

However, Dzazali, Sulaiman & Zolait stated that users did are rendered ineffective if the people who interact with information systems do not practice prudent information security; in other words, human factors must be considered. Policies or controls are considered ineffective if users are unaware of any security risks or the policies themselves.

Technology is rapidly developing in various countries such as Philippines, but they have been unable to apply the basics for information security. If students are to receive on-the-job training, data security is a crucial topic for them to learn to assimilate accountability and responsibility. Learning information security to develop fundamentals and needed to defend yourself opens the door to being vigilant and restraining you from thinking before clicking.

In the Philippines, they are trying to assess cybersecurity for better engagement on the data that users have assured safeguard. That is why the Philippines aims to boost the reliability and security of critical data to conform to data standards for protecting. Since the most likely to be attacked are those, who were trying to keep up with the Data Privacy Act, moreover, developed information security would most likely encipher protection and confirmation of complete security, with this kind of fundamentals recklessness and incompetence evaluated for any risk in an organization.

**Structure and Rationale of the Study**

Developing the fundamentals of information security is critical, especially now that we are in the grip of a pandemic. A significant proportion of employee and student data, such as self-identity, quality of work, and grade, are recorded online. However, our private data and information are now easily hacked. Hackers' techniques for stealing a user's character and using it for online fraud or other fraudulent activity are continually evolving. They may use many ad campaigns on social media, such as a link or a chance to win prizes, and many people may believe that it is valid. However, by clicking or going to that site, hackers will know concerning your location and other essential private information in just a minute.

Numerous people may be unaware that their personally identifiable information has been stored on the Internet and perhaps other sites. Lack of awareness of information security is a major concern. That is why it is essential to understand information security to practice or restrict the access, disruption, modification, disclosure, or breaches of security. Understanding information security helps reduce risk, preventing the loss of assets or Personally Identifiable Information (Information) and a large amount of your private data.

This research study aims to elaborate upon these risks involved with it by being unaware of information security. It also seeks to discuss the importance of security awareness to students by collecting information and asking research question to our respondents. This thesis will explain why developing the fundamentals of information security is essential.

**Statement of the Problem**

Given that information, security is a wide-range subject that is inexplicably complex to the students, much more complicated to understand practices amid time. The topic consists of fundamentals, technicality, and application-based scenario-based. The researcher needs a clearer picture of how the students will develop basic fundamental about information security and know more about their hindrances and challenges pursuing prima cognition to information security.

With this study, a clearer picture will be given to the students unaware of the topic and be knowledgeable before entering into a technical and application study in their on-the-job training.

This study will seize to answer the following questions:

(1) Can the students develop fundamentals to information security?

(2) How can the students learn information security?

(3) What practices need to apply?

(4) Is this beneficial to students, teachers, and school organization curriculum?

(5) How can these concepts and fundamentals help students?

(6) Were they able to apply it before approaching on-the-job training?

(7) Are there hindrances to pursuing information security subjects?

(8) Is there a chance they will be confused entering on-the-job training after they learned the information system?

(9) How can they behave after undergoing information system subjects/topics?

**Objectives of the Study**

The researcher’s main goal is to "develop fundamentals of information security for CARD-MRI Development Institute BSAIS students."

This research aims to help students become a little more aware of the digital world and showcase the importance of the information security subject—students during their first to the third year of BSAIS at the CARD-MRI Development Institute in specific.

Specific objectives;

To developed their prima cognition to information security.

To determine how students developed their selves in information security

To gain familiarity with information security technical terms

Determine the performance of the students to the subject.

Determine the significant difference in performance in

Technicality & Fundamentals

To establish convenience to the students

Determine the programs that will help students to understood information systems more

To understand significant risks and threats in information security

To find out their credibility and changes after learning information security.

To assess and identify any challenges in understanding information security.

To develop information security discipline and behavior

To have a better flow in understanding complex and complicated information security works

To identify some issues and concerns on the subject of information security.

**Significance of the Study**

This research study aims to provide information and knowledge to the beneficiaries about the selected topics from the respondents, recent studies as well as research, and related sites needed for such expected importance to the participants are as follows;

**The Future Researchers**

This research will benefit the future researcher to establish their own criticism and knowledge on how they will integrate students who are not aware of information security. This will be their guidelines and reference to find a way to help students understand more on information security.

**The Students**

The output of this research study will benefit the students who are not aware of information security, as they will be knowledgeable and understand the fundamentals of information security. This will be their basis on how they will be accountable, responsible and behave before going to fieldwork.

**The Teachers**

This will be very beneficial to the Teachers of Bachelor of Science in Accountancy Information System as they gave their own learning and experience to their students changing their perspective on this subject. Through this research, teachers will be the foundation for a new generation of teachers and students who are still newbies in AIS courses.

**Limitations of the Study**

The study focused on Developing Basic Fundamentals about Information Security for BSAIS students of CARD-MRI Development Institute. The primary subject of this research will consist of all Accounting Information System students starting from 1st to 3rd year as respondents. The limitation of the study includes gathering data online due to ongoing crisis of pandemic in the Philippines.

This study will not include students in their fourth year who have learned about information security and are undergoing on-the-job training. The same questionnaires will be given to each student to complete. The results of this study will be likely to apply to CMDI students and should not be used to find out the students' phase of development in Basic Fundamentals of Information Systems. The online questionnaire will be the primary data collection method.

**Definition of terms**

Software

A set of programs that tells computer to perform a task. that These instructions are compiled into a package that users can install and use. For example, Microsoft Office is application software.

Cyber Security

The efforts to design, implement, and maintain security for an organization's network connected to the Internet. It combines logical/technical-, physical- and personnel-focused countermeasures, safeguards, and security controls. An organization's cybersecurity should be defined in a security policy, verified through evaluation techniques (such as vulnerability assessment and penetration testing), revised, updated, and improved over time as the organization evolves and new threats are discovered.

Information Security

Information Security is the practice of preventing unauthorized access, use, disclosure, modification, inspection, recording, or destruction of information. Information can be a physical or electronic one.

Breach

The moment a hacker successfully exploits a vulnerability in a computer or device and gains access to its files and network.

Firewall

A defensive technology designed to keep the bad guys out. Firewalls can be hardware or software-based.

Malware

Any code is written for the specific purpose of causing harm, disclosing information, or otherwise violating the security or stability of a system. Malware includes a wide range of malicious programs, including viruses, worms, Trojan horses, logic bomb, backdoor, Remote Access Trojan (RAT), rootkit, ransomware, and spyware/adware.

DDoS (Distributed Denial of Service)

An attack that attempts to block access to and use of a resource. It is a violation of availability.

Hacker

A person has knowledge and skill in analyzing program code or a computer system, modifying its functions or operations, and altering its abilities and capabilities. A hacker may be ethical and authorized (the original definition) or malicious and unauthorized (the altered but current use of the term). Hackers can range from professionals who are skilled programmers to those who have little to no knowledge of the specifics of a system or exploit but who can follow directions; in this instance, they are called script kiddies.

Information Security Policy

A written account of the security strategy and goals of an organization. A security policy usually comprises standards, policies (or SOPs – Standard Operating Procedures), and guidelines. All hardware, software, facilities, and personnel must abide by the terms of an organization's security policy. (Also known as security policy.)

Risk Assessment

The process of evaluating the state of risk of an organization. Risk assessment is often initiated by taking an inventory of all assets, assigning each asset a value, and considering any potential threats against each asset. Threats are evaluated for their exposure factor (EF) (i.e., the amount of loss that would be caused by the threat causing harm) and frequency of occurrence (i.e., ARO—Annualized Rate of Occurrence) in order to calculate a relative risk value known as the ALE (Annualized Loss Expectancy). The largest ALE indicates the biggest concern or risk for the organization.

**CHAPTER II**

**REVIEW OF RELATED LITERATURE**

**Developing Basic Awareness practices on Information Security Overview**

**Information security awareness and behavior: a theory-based literature review**

(Benedikt Lebek, 2014) Currently, information systems are extremely important in today's organizations (IS). As a result, they put in place technical safeguards to keep information security dangers at a minimum (Aurigemma and Panko, 2007). Non-technical measures such as information security policies (ISPs) (Bulgurcu et al.,2010; Pahnila, 2007a, 2007b) and security education, training and awareness (SETA) programs (Abraham,2011; D'Arcy and Hovav,2009) are proposed as non-technical measures for preventing security breaches by employees in the literature. In part due to the fact that employees are often referred to as the weakest link in information security (Spears and Barki, 2010; Siponen et al., 2006), academic interest in employees' information security awareness (ISA) and behavior has grown significantly over the last decade. Several theories from social psychology and criminology were used to information security literature (Mishra and Dhillon, 2005) in order to explain and predict employees' security-related behavior and awareness, in this interdisciplinary research topic. There is still no current review of the hypotheses and main findings, despite the large number of studies that have been undertaken in this area.

We therefore offer the findings of a comprehensive literature review that was conducted in order to discover applied theories and comprehend cognitive determinants in the research field of employees' internal motivation and behavior during the previous decade in this paper. Siponen had undertaken a prior review of the literature (2000a, 2000b). Users-related problems in information security were investigated by the authors using a variety of methodologies. The study's focus was on approaches rather than the underlying theories, despite the fact that these were uncovered. Because the previous study was published 12 years ago, an up-to-date overview of applied theories is required to guide future research. The findings of Abraham (2011)'s literature review were based on elements that influence security behavior (such as policies, communication practices, peer effects, and so on), rather than theories. Several target-oriented literature reviews were also done as part of the research project. If the literature review was undertaken to give the theoretical basis for subsequent study within the same article (for example, model creation), it was considered "target oriented," which indicates that it was not considered an essential part of the article. Anomie theory was introduced into the research field by Mishra and Dhillon (2005), who provided a succinct survey of behavioral theories in information security literature. Another paper, by Aurigemma and Panko (2007), investigated behavioral theories in order to offer an ISP behavioral compliance framework (ISP Behavioral Compliance Framework).

Using the following research topic as a starting point, the purpose of this work is to present an up-to-date summary of applied theories:

RQ1. The question is, what theories have been recently employed in information security literature to describe employees' security-related awareness and behavior?

144 publications that deal with employees' security awareness and behavior theories were reviewed in order to provide an answer to this topic. The conclusions of this review are presented in the following parts. Academic databases were searched for relevant literature from 2000 to the present day, which was then assessed with an emphasis on applied theory and research methods, as well as other factors. Using the basic elements of four key applied theories, we develop a meta-model that describes employees' information security behavior in the workplace. A discussion of factors that have been proved to have a substantial impact on employees' security behavior or intents is offered by integrating the outcomes of past empirically tested research models based on adopted theories. In addition, additional criteria that have been exploited in the research domain are highlighted. In the discussion of the findings of the literature analysis, it is pointed out that there are gaps in existing research. There are also recommendations for future investigations that are made in relation to the research studies and the subject under consideration. The findings of our research can be used by practitioners to improve employees' security-related behavior, as well as by researchers to extend and improve the ISA and behavioral models that have been developed in previous research.

**Literature Review of Information Security Practice Survey Reports**

(Yang, Yaping, Supervisor: Prof. Siponen Mikko, 2018) With the progression of technological innovations, both large and small businesses are confronted with increased information security issues and challenges, such as cyberattacks—breach of security, security workforce, cyber threats, and risks, etc. This dissertation aims to comprehend the big picture of worldwide enterprises' cyber security. By reviewing annual information security questionnaires and looking for the most difficult parts of information security management, you can improve your security practice. The investigation is ongoing. Built using the general research method with a focus on providing an understanding of the current situation of the research topic and providing detailed information on the findings, the research questions are 1) what are the global enterprise's information security practices situations from the year 2008 to 2016? 2) What critical topics have been addressed mostly by security professionals? 3) what are the origins, components, obstacles, and improvements for critical topics?

The research source is a survey of cybersecurity practices. Published by consulting firms such as E&Y, PwC, Deloitte, KPMG, and others SANS, McAfee Labs, CERT, and other security organizations The investigation Each year's topics also included relevant academic research and industrial applications. Studies. The study discovered nine areas in which global enterprises performed worse than expected: management framework, security policy, and organizational structure. Information security, people management security, communication security, and operational security are significant factors. Management, access control, contingency planning, business continuity management, and compliance were considered. ISO/IEC 27002 standard is being used. The findings evaluated the topics' origins, components, obstacles, and developments.

This thesis bridged the gap between existing understanding of organizational data security and recommendations for future developments in terms of contribution. It underscores the concerns with information security management during the previous nine years. It provides standards for organizations to enhance their effectiveness. Vulnerabilities must be discussed, and practices should be improved with a specific focus. Meanwhile, the complete review provides detailed figures by year, which could be used as a reference to develop further 's cybersecurity investigation.

**Information security awareness and behavior: trained and untrained home users in Sweden.**

(Fu, Johanna Hammarstrand & Tommy, 2015) Today, we live in the digital society that has ever been in technology. The amount of data that is processed, preserved and communicated Information Security is a concern for both individuals and the community's world when both groups are given access to data daily. Such a society will necessitate a greater aspect of information security. Previous researchers who have addressed this issue contend that information security is the most crucial component in bringing up the total security level. Furthermore, mention education to elevate security awareness and, as a direct consequence, obtain a secure environment. This study wants to analyze the differences in security awareness among trained and untrained everyday users.

The analysis was conducted using a quantitative research method in the form of a survey. The distribution of questionnaires for self-completion There are many 162 research participants. Respondents who took part The conclusion was presented and evaluated with the help of the IBM SPSS software program. The findings indicate that the awareness. The proportion of trained everyday users is higher than that of untrained home users. Moreover, the discussion implies that the household users who have already participated in Initiatives to promote awareness, such as training and education, may not always apply. more security measures in their residence than those regarded as untrained middle-aged women.

As a result, this study suggests that increased awareness may be beneficial. Not still be the only factor affecting the user behavior, even though someone who has not been involved directly or indirectly in awareness-raising initiatives engages security measures, sometimes to the exclusion of all others to the same extent as those who have. This thesis could serve as the foundation for future research. Future research in the field, given that the study would be a comparative study of the variable’s confidentiality and security between skilled and unskilled home users. Where the discovered results do not completely agree with the previous research, raising awareness is true to be supplemented by other indicators. Other groups, such as internet providers (ISPs), should provide appropriate training. Banks. Perhaps the solution is to create and seek a prolonged information flow. Swedish current societal security culture might also result in deeper learning and understanding of security problems and establishing in-home users an opportunity to be involved and proactive regarding their information security behavior.

**Information Security Policy Compliance: Systematic Literature Review**

(Elsevier B.V., 2019, pp. 1216-1224) A document that ensures information assets and secures technology information with a specific procedure to support the organization's objectives is known as an information security policy [1]. Information security policy ensures the security of information assets and information technology by following a specific procedure to support an organization's mission and goals. Management support is critical during the implementation of information security policies. When support is obtained, the next challenge is ensuring that policies truly improve security [2]. Management will be compared to technical products; value policy efficiency is more difficult to achieve. This is always easier for technical products because statistics are frequently used to debate efficiency. Despite the fact that the organization had implemented a security policy, it was discovered that employees ignored the rules and engaged in unusual behavior. Policies are only as good as the paper on which they are printed or the bits in which they are stored if they are not followed. Policy compliance aims to ensure that organizational security standards are followed [3]. Previous research has been conducted in order to develop a model of user compliance with information security policies. Bulgurcu (2010) investigates rationality-based factors that encourage an employee to comply with ISP requirements concerning protecting information resources and organizational technology, arguing that compliance benefits, compliance costs, and non-compliance costs, which are beliefs about valuation as a result of compliance or non-compliance [4], influence employee attitudes.

Users did not realize the importance of adhering to security policies until incidents occurred and organizations were forced to incur additional costs as a result of non-compliance behavior. Phamz (2015) investigates the literature to determine the importance of user motivation, regulation, and user orientation toward information security compliance [5]. Various studies have been conducted to learn about information security compliance; the majority of studies are conducted to determine what factors influence user compliance behavior. There is clearly an inadequate approach and a lack of solutions to improve user compliance with information security policies. More information can still be explored to improve understanding of compliance and user compliance with information security policy.

As a result, a systematic literature review is required to identify trends and challenges from previous research. A successful systematic approach to stay focused during a literature review, specific research questions are required. As a result, this literature review identifies the most significant journals in the field of information security compliance and identifies trends and challenges in information security compliance. This paper is structured as follows: Section 2 discusses the strategies used to find primary studies and study selection criteria, as well as the research method used to produce a systematic literature review. Section 3 presents the statistics derived from the review data in the form of data extracted from the review data. Section 4 provides an analysis of the findings as well as recommendations for future research. Finally, in Section 5, you will find the conclusions.

**Variables influencing information security policy compliance: a systematic review of quantitative studies**

(Teodor Sommestad, Jonas Hallberg, Kristoffer Lundholm, Johan Bengtsson, 2014) Today, enterprises are concerned about information security, as there are multiple dangers to information assets, both internal and external. Formalizing and communicating an information security policy is a typical and highly appreciated security practice. The information security policy outlines the management's objectives, principles, norms, and guidance for employee compliance. The purpose of the information security policy, as briefly stated (ISO/IEC, 2009), is to "give management direction and support for information security." It should include information on the penalties for violating security policies, permissible use of computer resources, information security duties, and the training that employees of various categories should get. The fundamental premise is that adhering to an effective information security policy will result in an increase in the organization's information security level. Nonetheless, ensuring compliance with an organization's information security policy is anything but straightforward.

Organizational decision makers require assistance on the most effective methods for enforcing their information security policy and discouraging inappropriate behavior. Numerous studies have been undertaken on the subject, and the majority of them provide more information. The research examined a large number of variables that were derived from a variety of notable theories in the field of information systems. D'Arcy and Herath (2011) conducted an ad hoc review of a few research that were associated with one of these ideas (deterrence theory). Padayachee (2012) recently published a taxonomy of characteristics associated with compliant information security behavior based on an ad hoc analysis of a sample of the literature. However, no systematic evaluation of the findings from research on user compliance (or deliberate noncompliance) in general has been conducted. This article conducts a systematic review of empirically validated study findings with the goal of addressing the following questions: Which variables are critical for ensuring compliance with security standards? and What role do these variables play? The review will include all peer-reviewed studies that are publicly available on the subject.

This paper will follow the following outline. The second section details the methodology for conducting the systematic review.

**REVIEW OF RELATED STUDIES**

**An introduction to Information Security Practices**

**Information Security Management Practices: Case Studies from India**

(Singh, Abhishek Narain; M.P Gupta, 2017, pp. 253-271) Data protection has gained prominence in organizations and fields across the board. The major reasons nowadays are the new and creative methods of data managing (during the age of handling, stockpiling, and appropriation) and the reliance of organizational processes on current and innovative IT/ICT mediums in institutions to complete day-to-day business procedures. This has made associations more agile in terms of working while also presenting tough possibilities. To a certain end, the current review will investigate and examine the data security top management (ISM) practices of 2 different IT progression and administration policies organizations in India. If the study plan is accompanied, the review would include an open interpretation inspection course to comprehend the current ISM practices of the case associations. Perceptions obtained from semi-organized

Interviews are presented using an enlightening research technique. Furthermore, the SAP-LAP (Scenario, Entertainer, Cycle Acquiring knowledge, Activity, Execution) request technique is used to break down the findings from contextual investigations. The findings have important implications of predictable top-level administration support, a hierarchical data security culture, and a suitable checking guideline for ISM adequacy in organizations. The review's knowledge can be beneficial for managers and leaders in monitoring credible data security drills.

**Studies on Employees’ Information Security Awareness**

(Von vorgelegt, Felix Haubinger, Geboren in Munchen and Gottinger, 2015) The introduction of the TCP/IP Internet protocol in 1973, as well as the numerous connections made possible by technologies such as computing devices, smartphones, networks, wireless links, and other information technology (IT) infrastructure, have resulted in enormous progress. People and businesses all over the world are reaping the benefits and opportunities. The rapid advancement of Global networking and the societal penetration of information- and communication technologies

Technologies such as information and communication technologies (ICT) and an increasing reliance on information systems (IS) have had an impact. made critical infrastructure management (e.g., healthcare, energy, finance, etc.) logistics, administration, etc.) more efficient than ever before. But there is a darker side to this evolution, too. As a result of the connected world and because of their reliance on IS, private and public institutions have become increasingly an asset that is vulnerable to cyber-attacks, data theft, and the loss of critical business information which is regarded as the backbone of an organization (Qudaih et al. 2014). As Numerous high-profile incidents in recent years have revealed organizational flaws.

The security of information systems (ISS) can have serious societal and economic consequences.

economy. Cyber-attacks from outside the company, as well as insider threats and vulnerabilities

Employees' unintentional misbehavior can result in a wide range of consequences.damage, such as financial loss, loss of customers and business partners, decrease of the firm's market value, reputational damage, or even government sanctions (Goel andShawky 2009, PWC 2013). to a recent estimate by the Centre for Strategic and Think tank Center for Strategic and International Studies (CSIS), cybercrime, and intellectual-property theft causes an annual global loss of $445 billion – roughly the same as a country's GDP Austria is a smallish, wealthy European country (The Economist 2014). As a result, organizations around the world reportedly spent more than $ 67 billion on information

According to Gartner, security was a top priority in 2014 (The Economist 2014). Small and medium-sized businesses are expected to spend even more on information. security than on other IS/IT over the next three years (Perlroth and Rusli 2012). Previous attempts to ensure information security have largely focused on technological remedies, such as encryption, anti-spyware, virus detection, or firewalls (Stanton et al. 2005, Spears and Barki 2010) Investing in technological ISS countermeasures, however, is insufficient, because it is assumed that 50-70 percent of all information security incidents occur. Employee misbehavior in organizations, either directly or indirectly, causes a variety of problems. from careless errors to intentional harm (Ernst and Young 2003, (Siponen and Vance, 2010). Improving information security thus necessitates investments in both technical and human resources. as well as socio-organizational resources (Bulgurcu et al. 2010). Against this backdrop,

Scholars and practitioners have recently shifted their focus to the human dimension of information security by applying principles of behaviorism and social psychology. Employees' information security awareness (ISA) has been identified as a factor in this regard.be one of the most essential prerequisites of information security behavior and to play a key role in employees’ policy compliance (Siponen 2000, Dinev and Hu 2007, Bulgurcu et al. 2010, Al-Omari et al. 2012). ISA is most frequently referred to as a cognitive state of mind, which is distinguished by an understanding of the significance of information security and being aware of ISS objectives, risks, and threats, as well as having an interest in gaining the necessary knowledge to use IS responsibly (Straub and Welke) Thomson and von Solms 1998; Siponen 2000).

Individuals who have high levels of ISA, not only do they have a better understanding of information security risks, but they also have a better understanding of how to mitigate them. Also, make more effort overall to help keep company information secure (Siponen 2000). On the one hand, this means that employees defend the company's information against attacks and illegal information retrieval from outside the company. Whilst, on the other hand, it means that employees are less likely to take advantage of their easy access to information. corporate confidential information, thereby preventing them from becoming a threat that the company is trying to protect itself against (Straub 1990). ISA is respected as a highly significant indicator of organizational information's overall performance security management (ISM) practices (Hu and Dinev 2005, Choi et al. 2008) and a main Cavusoglu et al., 2009; Bulgurcu et al., 2010).

Also, ISO/IEC 27001 (2005, (2013) asserts that management responsibilities include ensuring that employees, contractors, and subcontractors are properly trained. and third-party users achieve a level of awareness about information security relevant to their roles and responsibilities within the organization Despite the fact that the importance of employee ISA has been widely acknowledged, recent studies show that ISA remains a problem. a contentious issue, and that most employees are unaware of security concerns, policies, and procedures (Pahnila et al. 2007a, Lim et al. 2010). Research Questions, Contributions, and Structure of the Dissertation. The goal of this cumulative dissertation is to broaden our field of knowledge. according to various aspects of employees' ISA As a result, it includes three. interrelated studies, each of which formulates a series of research questions directed at different aspects of the topic, and gives a separate detailed discussion of the findings and their implications for research and practice. The first study is an extensive review of the existing body of ISA literature, whereas studies 2 and 3 are quantitative empirical examinations of proposed research models addressing different gaps in ISA research. The first paper provides a synthesized up-to-date review of the current state of ISA. literature, with the goal of providing quick, structured access to the accumulated knowledge of ISA research, to provide implications for scholars and practitioners, and to reveal potential areas for further research (Webster and Watson 2002). 131 selected ISA Publications are identified and analyzed. Using open coding techniques based on grounded theory is a method for breaking down a topic into logical subcategories. A classification scheme is developed that categorizes five main objectives of ISA research. An overview table is provided that shows which publications address which criterion (1-5), whereas a single publication can cover multiple criteria. Figure 1 depicts the classification scheme of the ISA literature

**The Effect of a University Information Security Survey on Instruction Methods in Information Security**

(Frank H. Katz, 2005) On March 11, 2005, the names of 98,000 graduate students and applicants to the University of California, Berkeley vanished. Nobody hacked into the University of California's computer system. The names and social security numbers were saved on a laptop that was left unattended in a restricted area of the graduate division offices. The laptop was discovered in an office off a corridor that is normally locked when the receptionist is away, but the corridor was not locked on the day of the theft. The laptop was only left unattended for 30 to 60 minutes. A user receives a Web postcard via e-mail and inadvertently installs a Trojan horse onto his system, becoming a victim of a clever social engineering attack. The card has a spoofed sender address and appears to be from bluemountain.com. However, a link in each e-mail claims to take recipients to Blue Mountain's card pickup Web page, where they are asked to enter a unique card ID number provided in the e-mail. Victims who click on the link are directed to a number of websites that may contain malware or malicious software. A student living in a university dorm installs file-sharing peer-to-peer (P2P) software on her PC to download music from the Internet. Despite the fact that it is clearly against university policy, she does it anyway, downloading files onto her computer that may contain viruses, worms, Trojan horses, or spyware. In her university's networked environment, she may have opened a port on the school's firewall, giving the attacker the ability to attack the system by exploiting any vulnerabilities in the P2P application. Aside from possibly violating copyright and putting her university in legal jeopardy, she has unintentionally jeopardized her own confidential information, the secure data of others using the network, and the network's integrity.

Many people are afraid of online identity theft, even though many identity thieves do not profit online. Instead, they're rummaging through trash and stealing from easily accessible paper files. According to James Van Dyke, principal analyst at Javelin Strategy and Research in Pleasanton, California, friends, family members, and neighbors account for half of all known thieves and cost the victim an average of $15,607, compared to $2,320 for an online thief. "It's still so much easier to grab something from a desk or the trash," Van Dyke said. Over 2,400 years ago, Chinese General Sun Tzu said, "If you know the enemy and know yourself, you need not fear the outcome of a hundred battles." If you know yourself but not your adversary, every victory will be followed by a defeat. If you don't know your opponent or yourself, you'll lose every battle." His observation is particularly pertinent to information security in the twenty-first century.

All too often, when IT managers look to secure their organization, they focus on firewalls, routers, intrusion detection software, proxy servers, and the like. They may, however, be overlooking the most obvious problem in their organization, one that cannot be remedied by the most advanced software and hardware. They ignore their customers. As General Tzu would say, these managers don't know themselves – or their organizations. People are a part of the system, and failure to recognize this and address end-user training can lead to disaster. It is undeniable that "employees are one of the greatest threats to information security." Indeed, the 2004 Ernst & Young Global Information Security Survey "revealed that end-user security training was the No. 1 problem inside large organizations." Despite this, less than half of those polled said their companies had a formal training program in place to deal with the threat." A conference of Chief Information Officers from various companies and organizations in the Savannah area was held at Savannah Technical Institute on November 18, 2004. Participants were asked to list and then rank the issues confronting their organizations. Almost every attendee placed information security at the top of his or her priority list. The perceived lack of employee training in this discipline was a corollary to the problem of keeping information secure. Discussions among attendees emphasized the importance of training employees not only in technological security solutions but also in how to mitigate and prevent threats caused by people. Universities, which handle a significant amount of confidential information at any given time, are especially vulnerable to many of the purely human threats to information security. Intellectual property compromises, deliberate acts of theft, deliberate acts of information extortion, deliberate acts of sabotage and vandalism, and deliberate acts of espionage and trespass are some of these. Armstrong Atlantic State University (AASU) is no different than any other university. Professors and staff are responsible for safeguarding sensitive information ranging from student grades to faculty evaluations. It is critical that not only faculty and staff are trained in the proper behaviors required to secure information, but that Information Technology students are taught these as well so that they can participate in the development of information security programs after graduation. As a result, it is necessary to determine whether university faculty and staff are engaging in proper information security practices, and if not, how we can make recommendations to correct any flaws in our practices, best train our users, and incorporate these best practices into the pedagogy of our information technology courses as well as employee training.

I conducted an information security practices and behaviors survey among Armstrong Atlantic State University faculty and staff from February to April 2005. The survey questions assessed whether AASU faculty and staff were performing the simple everyday practices and behaviors required to avoid the threats to information security described above. The survey included statements about various information security practices, and users were asked to rate their agreement or disagreement with them on a scale of strongly agree to strongly disagree. The questions can be found in the Appendix.

It was critical to determine who would participate in the survey before distributing it to the Armstrong Atlantic State University community. It would be ideal if every employee, whether faculty or staff, did so. In reality, this would not be possible. It's unlikely that I could get every employee on a campus with over 600 of them to cooperate. I attempted to interview a cross-section of campus employees, ranging from academic departments across all colleges and schools to functional departments like the Registrar and Financial Aid. My initial plan was to send the surveys to the heads of the departments I chose, who would then distribute them to their employees. I requested that the surveys be returned to me by each respondent in order to maintain the anonymity of both the employees and departments. As a result, no department or individual will feel "singled out" as a result of potentially poor information security behaviors. However, as time passed, I decided to send the surveys to individual employees in departments that had not previously received them. Again, the fact that the response sheet did not include the respondents' names ensured their anonymity. 210 surveys were distributed, representing roughly one-third of AASU's faculty and staff. A little more than a third, or 73, of these were returned, with 50 being faculty and 23 being staff. Furthermore, 58 respondents have their own office, six shares an office, and nine work in a cubicle or open area.

**Statistical learning methods for information security: fundamentals and case studies**

(H.-K. Pao, Y.-J. Lee,C.-Y. Huang, 2014) One of the pillars of modern cyber technology has been information security. People wish for an intrusion detection system that detects intrusions automatically to ensure a secure system at all times. Statistical learning and machine learning algorithms were not widely used in information security applications until the last few decades. The traditional approach to information security research is heavily reliant on domain knowledge such as computer networks, databases, operating systems, and web technology. That is to say, regardless of how difficult it may be, mastering domain knowledge is a necessary condition for constructing a strong defense system to prevent intrusions into a domain or server. To detect an intrusion, we can solve a symbol matching problem with either an exact string matching [1] or an approximate longest common subsequence matching [2] algorithm. More broadly, we can use signatures to detect intrusive activities, which is known as the signature-based approach. On the other hand, we can use rule-based detection algorithms to distinguish intrusions from normal behavior.

Nonetheless, for both approaches, the blacklist for signature-based methods or the rules for rule-based methods may grow longer and longer over time, and performance eventually degrades as both time and storage requirements grow. In recent years, zero-day exploits [3] that take advantage of unsynchronized signature databases have frequently caused disasters due to infrequent patch updating. Furthermore, increases in the automation of intrusive procedures complicate detection rule designation and accelerate intrusion propagation. To summarize, for the traditional approach to work properly, we need experienced domain experts, a complete (which could be infinitely long) signature database, an efficient and effective detection method, and frequent and prompt signature updating to make the defense system work. The probabilistic approach is another method for dealing with the aforementioned issues. To compress the blacklist, we can use the probabilistic method to combine similar patterns that are generated along with some malicious activities into one group. A high-level guideline is to 'extract' knowledge from activity patterns and classify the intention behind the patterns as benign or malicious. A theoretical treatment includes using a Markov chain or hidden Markov model [4, 5] to model sequential data, which is a type of generative model in the sense that we can actually generate more sequential data (such as an attack sequence in a network environment) given the model.

A Probabilistic Graphical Model [6, 7] is a general model that can describe a dataset with various dependencies, including spatial and temporal dependencies. To detect intrusions, anomaly detection techniques can supplement the shortcomings of signature-based methods. Although signature-based methods that belong to a specific hypothesis in concept learning [8] may have high false-negative problems, most anomaly-based detection methods that belong to a general hypothesis may have relatively high false positives. In general, combining the signature-based approach and the anomaly-based detection approach should yield better results than using only one of them in intrusion detection [9]. However, effectively implementing this integration in real-world intrusion detection systems remains difficult. Making a final decision is especially difficult when two approaches yield contradictory results. Probabilistic learning and anomaly-based detection techniques, both of which belong to the data-driven approach, are two examples of statistical learning methods that can be useful in solving information security problems. Statistical machine learning has gained popularity in recent decades as a result of several successful stories in which learning algorithms have been applied to problems such as speech recognition [4], bioinformatics [10], face detection [11], and autonomous driving [12]. One reason for such success is the development of discriminative models, such as support vector machines (SVM) [13], whose goal is to separate data that belong to different patterns. For example, given some malicious and benign training data, we can train a model and use it to classify new incoming data into one of two categories, a process known as supervised learning.

The algorithms used in generative modeling and discriminative modeling are distinct, as are the goals they attempt to achieve and the applications in which they excel [14]. Numerous information security problems, particularly system security problems, have already been solved using statistical learning methods. This is because, by definition, a system security problem can be transformed into a clustering or classification task, such as distinguishing between benign and malicious activities. Researchers can focus more on analyzing the security problem itself and identifying the key point to solving the problem with well-developed learning methods. To our knowledge, Forrest et al. [15] are the first research group to propose using learning methods to detect intrusions. Numerous studies based on generative models [16–18] are then conducted to investigate the effectiveness of learning methods in solving security problems. Researchers have also used discriminative models to address security concerns. They used RIPPER [19, 20], decision trees [21, 22], and SVM [20, 23, 24] to solve various security problems. Researchers have demonstrated that learning methods can solve security problems; however, it remains difficult when, for example, the training dataset is unbalanced, data labels are not 100% accurate, or the training data is not representative.

Even with so many learning methods available in the public domain these days, it is still difficult to successfully apply the learning methods to real-world information security problems due to the gap between academic research and industrial deployment [25]. Many subfields of information security exist, including network security, software security, database security, identification/authentication, spam filtering, privacy preservation, and many others. Applying learning algorithms to those various problems may result in different difficulties, and we demonstrate how to deal with various problems given a diverse set of algorithms. In this article, we will demonstrate how and why machine learning methods can aid in the resolution of information security issues. We introduce the fundamental statistical learning concept and show how learning algorithms can be used to solve real-world problems.

Statistical learning methods, like any other method, have limitations. The key idea is to use the methods in appropriate domains, possibly in tandem with other methods such as the traditional approach, to create a robust and efficient problem-solving package. The remainder of this paper is organized as follows. Section 2 discusses a few well-known information security problems as well as issues that arise when using statistical learning methods to solve the problems. In Section 3, we introduce the fundamental statistical learning concept, followed by a set of guidelines for selecting learning and statistical methods for real-world security problems. Following that, in Section 4, we present some case studies, and in Section 5, we summarize our conclusion.

**Assessing Information Security management in Malaysian Academic Libraries**

(ROESNITA BINTI ISMAIL, 2012) ISec is the means and methods of protecting data from unauthorized access, change, misuse, and loss, as well as ensuring its availability when needed. Initially, ISec was primarily concerned with technical issues, and responsibility was delegated to technical experts (Solms, 2000). As management becomes more aware of the importance of ISec, aspects such as policies, procedures, and top management involvement are incorporated into ISec management (Solms, 2000). As a result, it was felt that some form of standardisation, best practices, certification, ISec culture, measurement, and monitoring of ISec in an organization was required. Finally, views include the development of ISec governance as an integral part of corporate governance, which includes stakeholder commitment, proper organizational structures for enforcing good ISec, user awareness and commitment to good ISec, as well as the necessary policies, procedures, processes, technologies, and compliance enforcement mechanisms (Solms, 2006). ISec management in the context of library management refers to the controls that a library must put in place to protect its information assets from all potential threats in order to ensure the confidentiality, integrity, and availability of its information resources.

All libraries have information assets that must be safeguarded. In the library's IS, there are endless volumes of main resources, services, and personal patrons' records such as their names, addresses, e-mail addresses, passwords, loan records, and website logs, and most of these resources can be accessed remotely via the library website. According to Mohammed Imtiaz (2001), "library services must reach two readers through the use of technology in order to provide online access to globally generated information and to provide continuous worldwide access to library resources searchable from anywhere, at any time, by anyone." The increased reliance of libraries on the Internet for generating, collecting, organizing, presenting, and disseminating information and services has exposed them to a variety of threats. Failure to manage ISec properly may result in the library losing time, money, service delivery, and public trust. As Zimerman (2010) points out, library computers are physically vulnerable to malware agents such as Trojans, viruses, worms, adware, spyware, pornware, keystroke loggers, password stealers, as well as theft, damage, and destruction. External threats that libraries should be able to handle include hackers, viruses, worms, and Trojan horses (Al-Suqri and Afzal, 2007).

Thus, the primary roles of libraries in this digital environment are data availability, integrity, and preservation (Brainstorming Report, 2001). This thesis describes research on information security management (ISM) in Malaysian libraries. Many studies have focused on how to protect information systems (IS) from cyber threats, primarily from a technical standpoint. Other researchers have focused not only on technological aspects, but also on organizational ones (Calder and Watkins, 2003; Chan et al., 2005; Ma and Pearson, 2005; Mercuri, 2004 and Vaast, 2007). This study, on the other hand, was motivated by a desire to assess the types and statuses of technological and organizational measures used by academic libraries in Malaysia.

Some attempts have been made to comprehend the types of computer threats aimed at Malaysian health and industries, public offices, and workplaces. However, the types of threats that could breach library ISec remain unknown because very few empirical studies on ISec threats have been conducted specifically in a library setting. As a result, 3 this study aimed to investigate the perceived ISec threats, their frequency of occurrence, and the perceived main source of ISec threats in Malaysian academic libraries. The descriptive analysis revealed the status of implementation of technological and organizational measures in these libraries as well as the differences between these libraries in implementing technical and organizational measures due to the type of universities, years in ICT implementation, yearly ISec budget, availability of IS security staff, and availability of wireless through the sample obtained from key players of ISec in Malaysian academic libraries. The final outcome also provides empirical evidence on the most common types of hardware, software, workstation, data, hardware, software, data, network, physical, and human-related threats encountered by Malaysian academic libraries.

The first step in ISec planning is to understand which assets the library needs to protect and why they need to be protected. This necessitates an understanding of the various threats and vulnerabilities that confront a library's valuable assets. Security attacks such as hacking, denial of service, worms, and viruses frequently jeopardize the library's information security (Breeding, 2006). In most cases, the threat is directed at the information rather than the system that transmits it. However, precautions must be taken to protect the overall elements of the library IS, including the hardware, software, physical environment, documentation, and people associated with an IS, from any potential threats. And securing any of those elements in a library must be done without jeopardizing public services, user privacy, or legal access (Eisenberg and Lawthers, 2005). The potential consequences or impacts include a loss of information confidentiality, integrity, and/or availability. For example, security flaws in any library system can result in unauthorised access to confidential 4 information (such as patrons' personal information and circulation records) or loss of data integrity. These, in turn, can have a negative impact on publishers' or other content providers' trust, cause embarrassment or even economic loss to the library, and even lead to other serious problems if urgently needed information is unavailable (Fox and ElSherbiny, 2011).

Libraries serve a diverse clientele as a bridge between users and the universe of information resources, and there is increasing pressure on libraries to collaborate in providing access to services to members of other libraries or universities (Ahmed, 2000). As a result, libraries must have effective authentication mechanisms in place to ensure the privacy and confidentiality of information while it is being collected, stored, processed, and disseminated only to those who are authorized, such as library staff and registered members, and to prevent accidental disclosure of sensitive information. There are several security issues related to information confidentiality that are frequently overlooked in libraries (Newby, 2002; Cain 2003): 1) the privacy offered for data collected from patrons other than circulation records may be questionable; and 2) the risks of outside parties accessing circulation or other data from outside the library via an Internet connection and an unattended modem, or from staff who abuse their access rights, penetrating library systems. The consequences of unauthorised, unanticipated, or unintentional disclosure of confidential information can range from severe to serious, including: 1) jeopardizing library security due to the disclosure of Privacy Act data; 2) loss of public confidence, embarrassment, or legal action against the library; and 3) loss of collection or revenue due to an insecure computing environment (Stoneburner, Goguen and Feringa, 2002; and Cain, 2003). 5 Most library resources and services are now available at any time and from any location. Providing access to those valuable library resources via the library website may expose the library to greater risk because they can be accessed by people both inside and outside the library via the library server (Eisenberg and Lawthers, 2005). Libraries must decide how to protect the information stored, processed, transmitted, or accessed through library systems from viruses and worms in order to ensure that information and services are not corrupted, degraded, or modified without authorization, because intruders can come from anywhere in the world. A hacker was once reported to have defaced the website of the National Library of Australia, leaving a cryptic message on parts of the site. The defaced page was thought to have been posted on a Windows NT platform (McAuliffe, 2000).

The presence of contaminated, corrupted, or missing data may result in data violations, fraud, and successful attacks on system availability and confidentiality, lowering the assurance or integrity of a library system (Stoneburner, Goguen and Feringa, 2002). Breeding (2006) noted these scenarios as concerning remarks such as 'libraries are often perceived as "an easy mark" and become a jumping-off point for hackers to other networks or computers in a library.' It is critical for a library to use a dependable network system, to provide adequate workstations, and to provide flexible access hours from internal or remote areas. A library must also ensure that data and information are secure for authorized users, protecting them from denial of service (DoS), viruses, worms, and loss of IS capabilities due to natural disasters or human error (Eisenberg and Lawthers, 2005). If critical library IS such as online catalogues, online databases, and websites are unavailable to its end-users, the consequences are numerous and may include: 1) affecting the library's mission as an information provider; 2) losing revenue due to the loss of 6 system functionality and operational effectiveness of a library IS; and 3) losing productive time, thus impeding the performance of the library and its end-users. Obviously, the library ISM must at the very least ensure the confidentiality, integrity, and availability of information processed by an IS, as these are critical to the success of a library's administrative activities and services.

**CHAPTER III**

**METHODOLOGY**

**Research Design**

This study focuses on descriptive research design. To evaluate the variables in question, the descriptive method of research may involve the use of several other studies. It primarily uses quantitative data, though qualitative data is occasionally used for descriptive purposes. This research design is useful when not much is known about the topic or problem. Before you can research why something happens, you need to understand how, when, and where it happens. Descriptive Research Design was to evaluate and answered the Question “what” rather than the “why”, it practically observes the characteristics of the variable rather than controlling it. This research study will be collecting data at CARD-MRI Development Institute Bay, Laguna.

**Population and Sampling Procedure**

This study will use non-probability sampling methods used to combine convenience sampling and quota sampling. Convenience sampling means that the researchers chose the nearby and most convenient respondents to respond to the survey, and the data gathering continues until the targeted sample size is reached (Robson, 2011). In this study,

Convenience sampling was used to collect respondents from the first to third years of the Bachelor of Science in Accounting Information System curriculum. Quota sampling represents that the researcher selected respondents on objective to collect data. In order to achieve the study's purpose and be appropriate for answering the research question

Another problem related to a convenience sample is that it is often hard to generalize the findings due to unawareness of which kind of population the sample would be representative of (Bryman & Bell, 2015). This sampling procedure would seek to encourage all BSAIS students of CARD-MRI Development Institute as respondents

**Data Gathering Procedure**

The researchers take time to develop a questionnaire that is relevant to conduct this study. This study will include the goal of the survey questionnaires to the respondents as well as informing their credibility with full integrity as they answer significant questions. This will be fulfilled with comfort as the researcher inform that this survey will be confidential. Questionnaires composed of open- ended question as the students of CMDI will answer it in their own perspective.

**Data Analysis Procedure**

By pursuing information security management as an advanced subject from the BSAIS curriculum at CMDI, the findings from all interviews and questionnaires were gathered and analyzed. The findings would subsequently be used to determine the developmental stage of CMDI BSAIS students. All of these outcomes should meet the study's objectives.

This study used the following to analyze the data gathered: