INCORPORATING ISLAMIC PRINCIPLES IN INFORMATION SECURITY BEHAVIOUR: A CONCEPTUAL FRAMEWORK

OMAR BARZAK, NURUL NUHA ABDUL MOLOK*, MURNI MAHMUD SHUHAILI TALIB

Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Malaysia

**Corresponding author: nurulnuha@iium.edu.my*

(Received: 4th September 2019; Accepted: 19th September 2019; Published on-line: 30th November 2019)

ABSTRACT: *Information security behavior among employees has dramatically changed the organizational security threat landscape in recent years. This is due to the advancement of Information Technology especially mobile and social technologies which are seen to be blurring employees' professional and personal persona. Due to this, employees tend to perform information security behavior with and without intentions. However, current Information Systems Security literature indicates lack of distinction for the types of information security behavior among employees in organizations. This article aims to propose a conceptual model for categorizing and classifying the information security behavior to highlight the aspects of behavioral intention, compliance and severity. It is developed based on the integration of Islamic principles and contemporary studies in the relevant fields. Deep understanding of each classification in the conceptual model could provide research and industry with a clear definition and countermeasures for each identified behavior. This may lead to strategic and structured approaches to resolve and extricate the occurrence of the behavior.*

KEY WORDS: *Information Security Management; Organizational Security Behavior; Intentional Security Behavior; Unintentional Security Behavior; Information Security Countermeasures.*

1. INTRODUCTION

In today's interconnected environment, it is crucial for organizations to protect their valuable information from potential threats that are coming from inside and outside the organization. Many organizations pay much attention to external threats, such as hacking, intrusions and malware attacks, and focus on providing technical measures to prevent them (Colwill, 2009; Fernando & Yukawa, 2013). Although it is important to observe external threats, insiders have higher probability to affect the information systems (IS) more than outsiders. This is because they are inside the organization and have privilege to access organizational IS and information. Additionally, they may violate information security policies with or without intentions (Abdul Molok et al., 2013; Galvez, Shackman, & Guzman, 2015; Greitzer et al., 2014; Johnston, Warkentin, Mcbride, & Carter, 2016). For example,

Abdul Molok et al. (2013) report that most employees who posted sensitive information about the organization on online social networks had no intention to cause harm to the organization. Their behavior is perceived to be more unintentional in nature. In line with this, academia and organizations have started to change their scope towards focusing on insiders' behavior and their impacts on information security (Crossler et al., 2013). Indeed, humans are prone to misunderstandings and mistakes and they are considered as the weakest link in the information security chain (Crossler et al., 2013; Fernando & Yukawa, 2013). Similarly, according to Safa et al. (2015), human mistakes and poor information security practices are the main sources of information security breaches. Therefore, understanding the factors influencing insiders' security behavior can help organizations to control, monitor and predict employees' security behavior (AlHogail, 2015; Abdul Molok et al., 2013).

Despite security studies that focus on insiders' information security behavior, majority of them do not attempt to differentiate between insiders who have the intention to perform security breaches from those who have no intention to cause harm to IS (Alhogail & Mirza, 2014; Crossler et al., 2013). In fact, current studies do not provide comprehensive meaning to distinct different kinds of insiders' security behavior. However, understanding the differences between intentional and unintentional security behavior, and the factors influencing them is important for companies and organizations to apply different types of strategies and countermeasures to combat insider threats (Crossler et al., 2013). Bishop & Gates (2008) state that, insider threats are difficult to be detected since the definition and categorization of insiders often found to be inconsistent. In line with this, security studies agreed that a framework about insiders need to be established in order to effectively address behavioral aspect of the problem (AlHogail, 2015; Barzak et. al., 2016; CERT, 2013; Crossler et al., 2013; Fernando & Yukawa, 2013; Galvez et al., 2015; Ifinedo, 2014; Martin & Zafar, 2015). Furthermore, auditors, employers and managers can use this complete view of different types of insiders' security behavior in order to understand, observe and control security behavior such behavior (Predd, Pfleeger, Hunker, & Bulford, 2008; Safa et al., 2015; Stanton, Stam, Mastrangelo, & Jolton, 2005).

While contemporary security studies lack of security behavior definition and coverage on unintended security behavior, Islam has a clear definition of different categories of human behavior. Similar to academic studies, Islam views that human behavior is driven by human's intention. In Islam, if the behavior occurs without the intention to cause detriment to people, it is not accounted for. In line with this, the objective of this study is to provide different kinds of insiders' security behavior by referring to Islamic principles; looking at how Muslims' behaviors are categorized. By integrating the Islamic principles with contemporary security studies, this article proposes a categorization of security behavior among employees and defines each categorized security behavior. Additionally, it emphasizes the strategy of reward and punishment which can be derived from the proposed integrated model.

2. RESEARCH BACKGROUND

Whitman & Mattord (2013 p. 4) define information security as "*The protection of information and its critical characteristics (confidentiality, integrity and availability), including the systems and hardware that use, store and transmit that*

information, through the application of policy, training and awareness programs, and technology". Accordingly, the effectiveness of information security in organizations relies on three components which are people, process and technology (Hamill, Deckro, & Kloeber, 2005; Herath & Rao, 2009). In accordance to Martin & Zafar (2015) and Wybourne, Austin, & Palmer (2009), technical-control mechanisms are very important to protect the information assets and to record organization's processes. However, it can be useless if those who are administering these mechanisms are negligent, do not adhere to security policies or use their privileged access to harm IS and networks. Therefore, organizations need to have a comprehensive approach that combines people, technology and process in order to protect their IS assets (AlHogail, 2015; Furnell & Thomson, 2009; Ifinedo, 2014; Schultz, 2005). This article focuses on human aspects in protecting organizational information security behavior.

2.1. Insiders' Security Behavior

Considering that humans are the weakest link of the information security chain, it is observed that the trend of security studies is now moving towards examining insiders' security behavior and their impact on IS (Crossler et al., 2013; Guo, Yuan, Archer, & Connelly, 2011; Kreicberga, 2010). Brackney & Anderson (2004, p. 10) define insiders as, "*Anyone with access, privilege, or knowledge of information systems and services*". Indeed, insiders have more advantages and potentials to cause harm to IS over the outsiders because they are already inside the organization, bypassing the physical or network perimeter and have direct access to the IS (Colwill, 2009). They have the knowledge about organization and available assets that outsiders know nothing or little about it (Colwill, 2009). Moreover, insiders can target the information directly without facing the barriers that are faced by external hackers (Guo et al., 2011). Furthermore, insiders may unintentionally reveal confidential information due to lapses, negligence, carelessness and ignorance (Alhogail & Mirza, 2014; Bulgurcu, Cavusoglu, & Benbasat, 2010; Fernando & Yukawa, 2013; Galvez et al., 2015).

Predd et al. (2008) suggest that in order to address insiders' issues we have to know first who are the insiders, what kind of their actions that put IS at risks and how can we mitigate their risks to IS. Cole (2008, p. 38) elaborates on insiders' issues and their organizations when they do not pay more attention to them:

"*The insider threat is like a tumor. If you realize there is a problem and address it, you will have short-term suffering but a good chance of recovery. If you ignore it, it will keep getting worse and while you might have short-term enjoyment, it will most likely kill you*".

Insiders are always known as the weakest part of the information security chain. However, security studies that investigate the factors influencing end users to perform different types of security behaviors are still limited (Crossler et al., 2013). Therefore, this limited number of studies call for more research to cover different types of insiders' information security behavior. These types of behavior can be further used to classify individual security behavior with relevant methodologies and theories. In this way, organizations will be able to identify each categorized security behavior of their insiders in order to address the impacts resulting from certain types of security behavior (AlHogail, 2015; Galvez et al., 2015; Martin & Zafar, 2015). Following this stance, effective security policies and procedures to protect IS from

insider threats can be formulated effectively through the identification of intentional and unintentional types of security misbehaviors (Crossler et al., 2013; Abdul Molok et al., 2013).

One of the earliest studies that provide a taxonomy of human threats to IS is the study by Loch, Carr, & Warkentin (1992). Their taxonomy consists of four categories: i. external threats (human), ii. external threats (non-human), iii. internal threats (human) and iv. internal threats (non-human). Then, Warkentin, Straub & Malimage (2012) extend this taxonomy of IS threats by having three categories of insider threats: i. passive (non-volitional, non-compliance), ii. volitional (not malicious, non-compliance) and iii. intentional (malicious and harmful, computer abuse). Warkentin et al. (2012) suggest that in order to understand insiders' motivations, future studies should be conducted for each category. By doing this, organizations can detect and deter detrimental insiders' behavior earlier. Warkentin et al. (2012) also emphasize that each insiders' security behavior must be studied separately with appropriate methodologies and theories.

The importance of identifying different categories of insider security behavior is also felt by the security industry. Verizon (2012) provide the categorization of insider actions which comprises of three main classes: i. insiders who perform security behavior deliberately and maliciously, ii. insiders who perform security behavior inappropriately (but not maliciously), and iii. those who perform security behavior unintentionally.

Despite the above categorizations of insider security behavior from both academia and industry, there is still a gap in terms of the contributing factors that influence such behavior. Hence, this article attempts to fulfil this gap.

2.2. Employees' Intentions and Behavior

Martin & Zafar (2015) state that behavior is a complex interaction between conscious and unconscious mental processes. They also posit that the brain controls human's behavior in three different modes namely, Pilot mode, Autopilot mode and Co-pilot mode. Pilot mode represents behavior that is controlled by a fully conscious mind. Autopilot mode describes habitual behavior that is done repeatedly without thinking or conscious mind. Co-pilot mode represents behavior that is controlled by certain rules and policies in a stable environment but can be changed in certain situations. In accordance to the authors, most human's behavior is generated from unconscious mind or Autopilot mode. The weaknesses of human being appear when highly complex behavior of conscious mind becomes habitual behavior after repetitions. Therefore, the high level of habituation can unconsciously create greater information security threats.

Nowadays technology is changing human behavior in a different way so it is difficult to be predictable and expectable (Wybourne et al., 2009). Therefore, organizations need to understand the roles that technology plays in human behavior in order to enhance the security of IS (Wybourne et al., 2009).

Stanton et al. (2005, p. 2) mentioned that "*Appropriate and constructive behavior by end users, system administrators, and others can enhance the effectiveness of information security while inappropriate and destructive behaviors can substantially inhibit its effectiveness*". Additionally, Warkentin et al. (2012, p. 2) stated that: "*Each individual behavior and its antecedents must be analyzed*

differently with appropriate theoretical and methodological lenses". Hence, there is no one solution that can fit all issues that are related to human behavior.

2.2.1. Intentional Security Behavior

Intentional security behavior refers to information security behavior that is performed consciously or with intent. Employees are responsible for their actions, either good or bad since they intend to perform the behavior. However, in existing security studies, this type of behavior only describes malicious insiders who have full intention to cause harm to IS. For example, (NCCIC, 2014, p. 1) defines intentional security behavior as,

"*A current or former employee, contractor, or other business partner who has or had authorized access to an organisation's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organisation's information or information systems*".

Insiders are always trusted by their organizations and they have full access to the organizational IS (Colwill, 2009; Grimes, 2010; Warkentin & Willison, 2009). Indeed, insiders have the privileges that allow them to commit crimes in their workplace without leaving any evidence (Colwill, 2009; Grimes, 2010; Warkentin & Willison, 2009). What makes malicious insiders dangerous is that they can achieve high impact without leaving any trace to be discovered (Colwill, 2009; Fernando & Yukawa, 2013; Grimes, 2010).

In accordance to NCCIC (2014), there are some cases where malicious insiders try to recruit others by knowing their weaknesses and needs. Thus, organizations should be able to detect the recruitment signs and react quickly to prevent any suspicious employees from breaching their IS.

Colwill (2009) states that opportunity, capability and motivation are mostly the main factors of malicious insiders to perform their attacks. Opportunity and capability are controlled by organizations while motivations usually come from employee himself. Insiders have different motivations to engage in malicious behaviors such as, financial gain, personal gain, ego and some perform it because they know how to do it (Liu, Wang, & Camp, 2009). However, organization can easily control intentional security behavior by studying, monitoring and observing the factors that influence malicious insiders to involve in such behavior (Fernando & Yukawa, 2013). Moreover, organizations that enforced the desired information security behavior by having suitable information security's work environment and clear policies may be able to control malicious insiders' hazards (Colwill, 2009).

2.2.2. Unintentional Security Behavior

This section describes information security behavior that is done without employees' intentions. Unintentional information security behavior explains the actions that are performed by employees without their conscious or intentions and are done quickly and spontaneously without any thinking. It is very difficult for organizations to control this behavior as it is performed without employees' consciousness (CERT, 2013). Some studies have misconceptions when defining unintentional information security behavior when they consider intended security behavior that is done without malicious intent as part of unintended security behavior. Nevertheless, the right definition of unintentional information security behavior could be the behavior that is performed by employees quickly,

spontaneously and unconsciously which can be harmful or helpful to organizational IS. It means unintended security behavior occurred accidentally without employees' control and intentions. Even though there are many studies focus and cover intended information security behavior, security studies that cover unintended information security behavior are still scant (Alhogail & Mirza, 2014; CERT, 2013).

According to Abdul Molok et al. (2013), security incidents caused by employees are often unintentional in nature rather than intentional. They posit that most security breaches, particularly information leakage incidents, happen due to human mistakes and accidental security behavior that could cause more harm to IS. Similarly, the CERT Division of Software Engineering Institute, Carnegie Mellon University states that the main cause of unintended information security behavior is human error. Other studies suggest that there are some factors that affect these mistakes and errors such as security culture, organizational processes, management and security practices (CERT, 2013; Greitzer et al., 2014; Harrell & Harrell, 2014).

Examples of unintentional security behavior are sending an email to an unintended recipient, handling confidential data to unauthorized person mistakenly, selecting a simple password, unintentionally posting confidential data onto unsecured platforms such social networking sites, or visiting non-work related websites (Crossler et al., 2013; Safa et al., 2015). From these examples, we can see that employees might not have the intention to put IS under risks. However, these actions are leading to information security breaches and those negligent insiders are responsible for their actions.

According to CERT (2013), human errors and mistakes are the main factors of involving in unintentional information security behavior. Additionally, human errors and mistakes are affected by the security culture of organizations, organizational processes, management and security practice.

Moreover, employees are easily tricked by spear phishing, collusion from insiders or social engineering to reveal confidential information to others (NCCIC, 2014). According to NCCIC (2014), malicious insiders do not work independently. They usually tend to target weak employees or innocent insiders in order to collect confidential information from them unintentionally. The motivations and values given to the employee play very important roles to avoid unintentional security threats and prevent them to react improperly (Wybourne et al., 2009).

2.3. Se Security Behavior Theories

In order to understand the mentality of employees to involve in such security behavior, the researcher has studied some related behavioral, sociological and organizational theories to choose the suitable theories that can explain the phenomena.

1.3.1. Theory of Planned Behavior (TPB)

The theory was proposed by Ajzen (1991) to explain human intentions to perform such behavior. This theory explains the changes in human's behavior, attitudes, thoughts, actions, and feelings after interactions with other individual or group (Ajzen, 1991; Ifinedo, 2014).

According to Ifinedo (2014), TPB is widely used to investigate information security's ethical behavior and also the employees' decision to comply with information security policies and procedures. Therefore, the researcher chooses TPB to investigate intentional information security behavior where employees are fully aware of their actions and behavior towards IS.

1.3.2. Neutralization Theory

Vance & Siponen (2010) proposed their model based on Neutralization Theory (Sykes & Matza, 1957) to investigate why employees violate the policies of information security. The model of Neutralization Theory suggests that employees rationalize their violations of security policies by using a number of neutralization techniques, and these techniques offer a way for person to use existing norms to justify behavior that violates those norms. This theory is used to investigate intentional information security behavior without malicious intent (insiders who do not have the intention to cause harm. However, their action lead to breach the IS). In fact, some constructs of neutralization theory can also explain some techniques used by employees to make excuses after involving in unintentional information security behavior.

1.3.3. Intuition and Reasoning Theory

This theory can explain why employees involve in both intentional and unintentional (accidental) information security behavior. Kahneman (2003) mentions that, the brain of human is governed by two systems, intuition (System 1) and reasoning (System 2). Intuitions' system is fast and reflect the quick action of human when they perform it without any thinking (Kahneman, 2003). In this system, human's thoughts perform the action immediately without any effort of thinking and the decision is taken while human brain is affected by emotion and feelings (Kahneman, 2003). Therefore, this system is related to poor performance and mistakes by employees that can reflect unintentional information security incidents in this research.

On the other hand, reasoning system is slower, conscious and effortful. In this system, human are fully conscious and their mind is fully controlled while taking actions. Therefore, this system is responsible for intentional information security behavior whether good or bad. Hence, it is advices that unintentional information security incidents can be mitigated by motivating the conscious mind of the employees.

2.4. Behavior and Actions According to the Islamic Principles

Islam is the religion which affirms that there is only one God, the Creator of the universe and mankind. The main sources for Islamic law are the book of the words of God which is the Quran and the words of the prophet Mohammed which is called Hadith (Farooq, 2013). Intended and unintended actions and behavior are clearly distinguished in Islam because all Muslims' actions are considered valid or void depending on human's intention (Niyyah) to perform the action (Barzak, Abdul Molok, Talib, & Murni, 2016). Hence, the Qur'an and Hadith state clearly the rules and regulations to control intentional and unintentional behaviors and actions.

The importance of intention (Niyyah) in Islam is that, Muslims are requested to be aware and conscious of their actions and behavior as they are responsible of

what they do (Abdulsalam, 2006). The Hadith was narrated by Umar ibn al-Khattab who said: I heard the prophet Mohammed say:

"*All actions are judged by motives, and each person will be rewarded according to their intention*" (Abdulsalam, 2006). Therefore, involving in unintentional behavior or repeating the same mistake twice are discouraged in Islam (Barzak et al., 2016). Prophet Mohammed was encouraging his companions to avoid repeating their mistakes when he said: "A believer should not be stung twice from the same hole" (Sunan Ibn Majah, Book 36, Hadith number 3982). Meaning that Muslim should avoid repeating the same mistakes twice. Moreover, if any Muslim caused harm to other people or properties unintentionally, the offender must take full responsibility to fix all damages that he caused (Barzak et al., 2016).

Islam also requested its believer to fulfil their contracts and not to be involved in any actions that will break that contract intentionally or unintentionally. Moreover, it is obligatory for Muslims to seek knowledge and ask experts if they face any problems that could affect them to break the rules. Quran emphasizes that "…ask the people of the knowledge if you do not know" (Qur'an 16:43).

Hence, in order to control the intentional and conscious behavior of Muslims, there are five categories that serve as rewards and punishments for performing certain actions. Following Juned (2015), Islam draws the following categories of human behavior:

- Obligatory (Fard/Wajib): any action that you earn a reward for performing, and earn a punishment for abstaining from it. Examples include praying, fasting, etc.
- Recommended (Mustahab/Sunnah): any action that you earn a reward for performing, and earn nothing for abstaining from it. Examples include giving charity, smiling to others etc.
- Prohibited (Haraam): any action you earn a punishment for performing, and earn a reward for abstaining from it. Examples include theft, murder, and adultery.
- Reprehensible or discouraged (Makrooh): any action you earn nothing for performing, and earn a reward for abstaining from it. Examples include staying awake for late time at night.
- Permissible (Mubah): any action you earn nothing for performing, and earn nothing for abstaining from it. It is like daily social human behavior such as determining the food to eat or clothes to wear as long as it is within the limits set by religion.

3. CONCEPTUAL MODEL OF EMPLOYEES' INFORMATION SECURITY BEHAVIOR

Based on Sokolowski & Banks (2010, p. 3), a conceptual model is defined as,

"*A physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process. Simply, models serve as representations of events and/or things that are real (such as a historic case study) or contrived (a use case)*".

In fact, the conceptual model of insiders' security behavior (Fig. 1) is proposed based on our review of contemporary security literature and the Islamic principles. The conceptual model represents different kinds of information security behavior including both desired and undesired information security behavior. Therefore, each construct of information security behavior is clearly defined with assignment of rewards and punishments which were derived from the Islamic principles.

The underlying conceptual model in Fig. 1 consists of Intentional Security Behavior and Unintentional Security Behavior which are categorized into Compliance and Non-Compliance. Each category may be grouped further into Enforceable, Preferable, Preventable and Unacceptable. Each preventable behavior could be committed with malicious intent or without malicious intent.

As it is provided by Fig. 1 that information security behavior is categorized to intentional security behavior and unintentional security behavior as all human actions are governed by their intentional and unintentional mind. Kahneman (2003) mentions that human actions are governed by two systems. Intuition represents the first system is that is effortless and fast which can reflect unintentional human behavior. Reasoning represents the second system that is effective and slow which can reflect intentional human behavior. The underlying conceptual model in Fig. 1 consists of Intentional Security Behavior and Unintentional Security Behavior which are categorized into Compliance and Non-Compliance. Each category is grouped further into Enforceable, Preferable, Preventable and Unacceptable. Each preventable behavior could be committed with malicious intent or without malicious intent.

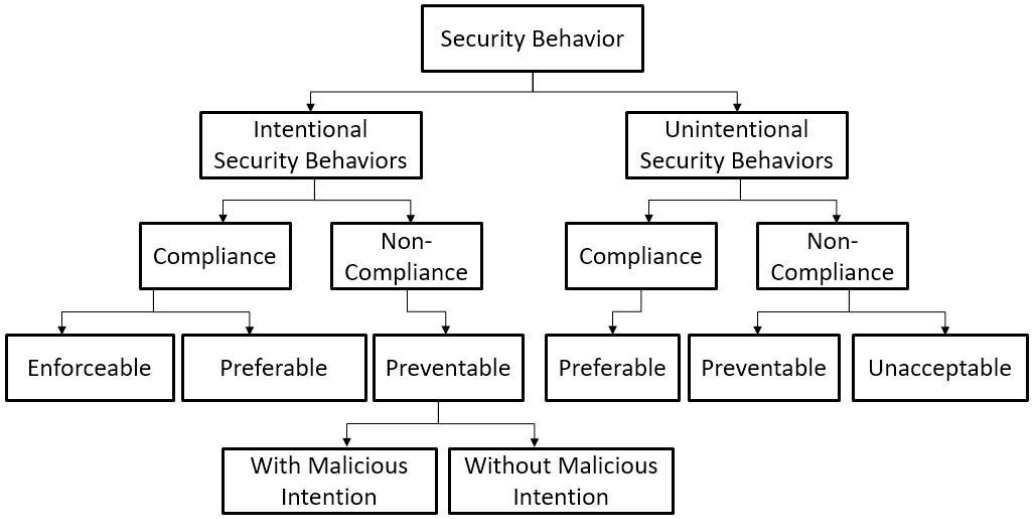

Fig. 1. Conceptual Model of Information Employees' Security Behavior.

The forth level of Fig. 1 shows different kinds of information security behavior that are Enforceable, Preferable, Preventable and Unacceptable behavior. These behaviors are derived from the Islamic principles that were discussed in the previous section which can help organizations to assign their information security policies and the rewards and punishments' rules.

Enforceable behavior is derived from the obligatory part of Islamic behavior and represents the behavior that should be enforced by the organizations. Therefore, organizations should enforce the information security rules, procedures, policies and standards that employees must follow them. However, failing to follow these policies and instructions is prohibited either with or without intention. It is as the same concept of Islamic principles that when employees comply with information security policies and procedures, they are not going to be rewarded because it is obligatory and they must follow them. However, failing to comply with information security behavior with or without intention would lead to punishments and sanctions according to what have been stated in the information security policies.

Preferable behavior is derived from recommended part of Islamic principles and shows any desired behavior that is preferred by organizations to increase the information such as; suggesting information security practices to the top managers, helping others to comply with information security policies and procedures, following information security guidelines and reporting any suspicious case. Preferable behavior can be performed with or without employees' intention. Therefore, employees who performed the preferable behavior should be rewarded.

Preventable behavior indicates the prohibited part of Islamic principles and covers information security behavior that organizations must warn their employees to avoid it. These behaviors can be represented as the malicious intention of employees to cause harm to IS, or those their actions affect the security of IS as they did not comply with information security policies and procedures. It is advised that employees who involve in preventable behavior should be punished.

Unacceptable security behavior is derived from discouraged part of Islamic principles and represents the behavior of employees who involve in information security behavior without intention. However, the impact of this behavior to the information security might appear in the long run by exposing IS to the threats. The probability of employees to involve in preventable security behavior increases if they involve much in this behavior. Additionally, organizations need to monitor and observe unacceptable security behavior to respond immediately before any loss or damage to organizational information. In addition to that, this behavior can be reduced by designing suitable organizational security policies with rigor countermeasures. Employees should be warned to mind their behavior and not to involve in unacceptable security behavior because it reflects a poor security practice. An example of this type of behavior is leaving unencrypted hard drive which contains confidential information on the table after completing the tasks that can be reachable and observable by others. As reflected from the Islamic principles, those who avoid involving in such unacceptable security behavior should be rewarded.

Each categorized behavior in Fig. 1 is explained below:

- Enforceable Compliance of Intentional Information Security Behavior:

For this category, organizations ensure that employees comply with information security procedures, policies and rules. Organizations need to have information security policies that are well documented, implemented and enforced. They make sure that their employees are fully aware of their responsibility to protect organizational information. In order to achieve this ideal category, organizations are

encouraged to know the influencing factors that affect employees to comply with their information security policies and have good information security behavior.

- Preferable Compliance of Intentional Information Security Behavior:

This behavior represents the behavior that organizations should encourage their employees to perform in order to strengthen the information security such as, following the guidelines of the information security that make information is well-protected. For example, encrypting all confidential information, locking the screen when leaving the office and organizing and arranging the information based on their confidentiality. Organizations should provide rewards for those who perform behavior that increase their information security.

The second part shows non-compliance with information security policies with or without malicious intent.

- Preventable Non-compliance Behavior with Malicious Intention:

It represents the employees' malicious behavior that they do it with the intention to harm organizational information system for many reasons such as personal and financial gain, their ego, their friends and others. By realizing that employees may fall into this category, organizations should have clear policies and procedures to prevent such behavior. Moreover, employees should be warned of the consequences of involving in such behavior.

- Preventable Non-compliance Behavior without Malicious Intention:

This part covers the organizations' procedures to prevent employees' behavior that is done with intention. The non-compliance security behavior happens due to carelessness, ignorance and negligence of the employees. Although there are many arguments about this behavior whether it is under intentional or unintentional security behavior, we believe that it is intentional as employees are aware of their actions, but they do not think or mean to cause harm to organizational IS. Organizations should give education, awareness and training programs to make employees aware of the consequences of such behavior. Punishment should be placed to employees who perform that behavior. For example, an employee did not comply with an information security policy i.e. sharing user account and password with colleagues in order to meet a work deadline.

Unintentional information security behavior is behavior that employees are doing it spontaneously, unconsciously and quickly that can help or harm organizational IS. In fact, it is very hard for organizations to control unintentional information security behavior so that it needs a high focus to be controlled.

- Preferable Compliance of Unintentional Information Security Behavior:

It represents the helpful behavior that can be defined as, any unintentional information security behavior that can increase the level of organizational information security. Such as, immediate closures of the screen's display while he was looking at confidential data and unauthorized person has entered his office. The unintentional security action of the employee represents high compliance to information security as he did not want that unauthorized person to look at it. These kinds of information security behaviors are performed with unconscious mind, and after performing these security behaviors more often, they become habit for

employees. Organizations should award their employees who perform such behavior because it represents very high level of information security compliance.

- Preventable Non-compliance of Unintentional Information Security Behavior:

It represents the procedures that organizations should have to prevent employees from involving in disruptive behavior unintentionally that can badly affect IS security. For example, sending a strategic plan to organization's client instead of the top managers mistakenly.

- Unacceptable Non-compliance of Unintentional Information Security Behavior:

This category represents employees who are involved in information security behavior that is performed without the intention to cause harm to organizational IS. However, there could be an impact of their behavior that can lead to information security breaches in the long run. This behavior may increase the probability of employees to be involved in non-compliance behavior. For example, misplacing an external hard disk drive or USB flash drive that carry confidential information after using them.

Studying these different types of behavior and the factors influencing them can be very helpful for organizations to have a comprehensive understanding of their insiders' behavior. Therefore, organizations will be able to monitor, observe, detect and control information security behavior of their insiders. For example, organizations should impose strict security policies if they realized that many employees are doing preventable non-compliance behavior. Additionally, organizations should focus on security education and awareness if the majority of employees are involving in unacceptable non-compliance of unintentional information security behavior. In accordance to CERT (2013), organizations can control intended information security behavior. However, unintended information security behavior is difficult to be detected and controlled. They also posit that organizations need to be vigilant about different types of such behavior in order to address it.

4. DISCUSSION AND CONCLUSION

The conceptual model is designed to provide academic and organizations with a categorization of information security behavior based on the integration of Islamic principles and contemporary security studies. It also emphasizes on the use of rewards and punishments to each type of categorized security behavior based on Islamic teachings. The main reason to include Islamic principles is Islam rewards or penalizes human actions based on their intention and it disregards bad actions that are done without the intention to cause harm to someone or something. Furthermore, Islam clearly outlines five categories of human behavior. Consequently, we adapted these categories together with taxonomies from contemporary security studies to propose our theoretical model of information security behavior.

Although current security studies and information security models mostly focus on non-compliance information security behavior, our proposed framework covers both compliance and non-compliance information security behavior. Therefore, our

study calls for more research in identifying the factors influencing security behavior in order to stimulate good behavior and decrease bad behavior. Security researchers can investigate different theories and suitable methodologies, and different security impacts of each categorized behavior. Furthermore, they can use the framework to identify the security impact and severity level information security behavior that is done with or without intent.

The proposed model can be effectively used in organizations to address different types of employees' security behavior. In fact, these behaviors are varied from one organization to another. Hence, the model would help organizations to analyze, understand and interact to their employees' security behavior by assigning different security measures and implement information security policies that suit and cover all aspects of their employees' security behavior

This article is considered as timely and important due to the current security researchers' and the industry's attention given to the behavioral aspects of information security.

REFERENCES

Abdul Molok, N., Chang, S., & Ahmad, A. (2013). Disclosure of organizational information on social media: Perspectives from security managers. *The Pacific Asia Conference on Information Systems (PACIS) 2013 Proceedings.108.*

Abdulsalam, M. (2006). ACTIONS AND INTENTIONS (PART 1 OF 2): PURITY OF INTENTION IN THE RELIGIOUS REALM.

Ajzen, I. (1991). The theory of planned behavior. *Orgnizational Behavior and Human Decision Processes*, *50*, 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Alhogail, a., & Mirza, a. (2014). Information security culture: a definition and a literature review. *Proceedings of IEEE World Congress On Computer Applications and Information Systems*. https://doi.org/10.1109/WCCAIS.2014.6916579

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567–575. https://doi.org/10.1016/j.chb.2015.03.054

Barzak, O., Abdul Molok, N. N., Talib, S., & Murni, M. (2016). Unintentional Information Security Behavior from the Qur'an and Hadith's Perspective. *International Journal on Islamic Applications in Computer Science And Technology*, *4*(3), 1–10.

Bishop, M., & Gates, C. (2008). Defining the insider threat. *Proceedings of the 4th Annual Workshop on Cyber Security and Informaiton Intelligence Research Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead - CSIIRW '08*, 1. https://doi.org/10.1145/1413140.1413158

Brackney, R., & Anderson, R. (2004). *Understanding the Insider Threat*. *Proceedings of the March 2004 Workshop*. https://doi.org/QA 76.9 .A25 B73 2004

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empiracal Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523–548.

CERT. (2013). Unintentional Insider Threats : A Foundational Study, (August), 91. Retrieved from https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf

Cole, E. (2008). Addressing the insider threat with NetIQ security and Administration Solutions.

Colwill, C. (2009). Human factors in information security: The insider threat - Who can you trust these days? *Information Security Technical Report*, *14*(4), 186–196. https://doi.org/10.1016/j.istr.2010.04.004

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future Directions for Behavioral Information Security Research. *Computers & Security*, *32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Farooq, U. (2013). Sources of Islamic Law, Primary and Secondary Sources of Islamic Law.

Fernando, S. a., & Yukawa, T. (2013). Internal control of secure information and communication practices through detection of user behavioral patterns. *Lecture Notes in Engineering and Computer Science*, *2*, 1248–1253. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84887865960&partnerID=tZOtx3y1

Furnell, S., & Thomson, K. L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud and Security*, *2009*(2), 5–10. https://doi.org/10.1016/S1361-3723(09)70019-3

Galvez, S. M., Shackman, J. D., & Guzman, I. R. (2015). Factors Affecting Individual Information Security Practices, (2009), 135–144.

Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014). Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. *2014 IEEE Security and Privacy Workshops*, 236–250. https://doi.org/10.1109/SPW.2014.39

Grimes, R. A. (2010). Combating the enemy within. *InfoWorld Media Group*, (July).

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems*, *28*(2), 203–236. https://doi.org/10.2753/MIS0742-1222280208

Hamill, J. T., Deckro, R. F., & Kloeber, J. M. (2005). Evaluating information assurance strategies. *Decision Support Systems*, *39*(3), 463–484. https://doi.org/10.1016/j.dss.2003.11.004

Harrell, M. N., & Harrell, M. N. (2014). Factors impacting information security noncompliance when completing job tasks, (21).

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management*, *51*(1), 69–79. https://doi.org/10.1016/j.im.2013.10.001

Johnston, A. C., Warkentin, M., Mcbride, M., & Carter, L. (2016). Dispositional and situational factors : influences on information security policy violations. *European Journal of Information Systems*, (April 2013), 1–21. https://doi.org/10.1057/ejis.2015.15

Juned, A. A. (2015). What Mufti says about the terms Wajib, Sunnah, Haram, Makruh and Mubah. *THE BRUNEI TIMES*, 7. Retrieved from www.bt.com.bn/files/digital/Islamia/Issue334/BT30Jan.7.pdf

Kahneman, D. (2003). Maps of Bounded Rationality : Psychology for Behavioral Economics. *The American Economic Review*, *93*(December 2003), 1449–1475.

Kreicberga, L. (2010). *Internal threat to information security*. *Pure.Ltu.Se*. Luleå University of Technology. Retrieved from http://pure.ltu.se/portal/files/31184594/LTU-PB-EX-10050-SE.pdf

Liu, D., Wang, X., & Camp, L. J. (2009). Mitigating inadvertent insider threats with incentives. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *5628 LNCS*, 1–16. https://doi.org/10.1007/978-3-642-03549-4_1

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Systems : Reality , Today ' s Yesterday ' s Understanding, *16*(2), 173–186.

Martin, N., & Zafar, H. (2015). AMCIS 2015 Puerto Rico Paper Submission Information Security : Modeling the Unconscious Mind, 1–7.

Molok, A., Nuha, N., Chang, S., & Ahmad, A. (2013). Disclosure of organizational information on social media: Perspectives from security managers. *Disclosure*, *6*, 18–2013.

NCCIC. (2014). Combating the Insider Threat. *National Cybersecurity and Communications Integration Center*. Retrieved from https://www.us-cert.gov/sites/default/files/publications/Combating the Insider Threat_0.pdf

Predd, J., Pfleeger, S. L., Hunker, J., & Bulford, C. (2008). Insiders behaving badly. *IEEE Security and Privacy*, *6*(4), 66–70. https://doi.org/10.1109/MSP.2008.87

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*(MAY), 65–78. https://doi.org/10.1016/j.cose.2015.05.012

Schultz, E. (2005). The human factor in security. *Computers and Security*, *24*(6), 425–426. https://doi.org/10.1016/j.cose.2005.07.002

Sokolowski, J. A., & Banks, C. M. (2010). *Modeling and Simulation Fundamental, Theoretical Underpinnings and Practical Domains*. John Wiley & Sons, Inc. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=2528092A9DC03C5AB4B89FA37BED628C?doi=10.1.1.473.5394&rep=rep1&type=pdf

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security*, *24*(2), 124–133. https://doi.org/10.1016/j.cose.2004.07.001

Sykes, G., & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review*, *22*, 664–670.

Vance, A., & Siponen, M. (2010). Neutralizaiton: New Insights into the Problem of Employee Information Systems Security. *MIS Quarterly*, *34*(3), 487–502. https://doi.org/Article

Verizon. (2012). *2012 Data BREACH Investigations Report*. Retrieved from https://dti.delaware.gov/pdfs/rp_Verizon-DBIR-2014_en_xg.pdf

Warkentin, M., Straub, D., & Malimage, K. (2012). Featured Talk : Measuring Secure Behavior : A Research Commentary. In *Annual Symposium on Information Assurance & Secure Knowledge Management* (pp. 1–8).

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security : the insider threat, 101–105. https://doi.org/10.1057/ejis.2009.12

Whitman, M., & Mattord, H. (2013). *Management of Information Security* (Fourth edi). Boston: Information Security Professionals.

Wybourne, M., Austin, M., & Palmer, C. (2009). *National Cyber Security Research and Development Challenges. Related to Economics, Physical Infrastructure and Human Behaviour.* Retrieved from http://www.thei3p.org/docs/publications/i3pnationalcybersecurity.pdf