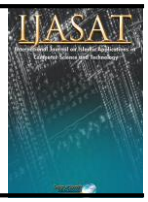

Unintentional Information Security Behavior from the Qur'an and Hadith's Perspective

Omar Barzak [1], Nurul Nuha Abdul Molok [2], Shuhaili Talib [3] and Murni Mahmud [4]

[1,2,3,4] Department of Information Systems (DIS), Kulliyyah (Faculty) of Information & Communication Technology (ICT), International Islamic University Malaysia (IIUM), Malaysia
[1]omar.mokhles@live.iium.edu.my, [2]nurulnuha@iium.edu.my, [3]shuhaili@iium.edu.my, [4]murni@iium.edu.my

Abstract

As the world becomes more interconnected now than decades ago, information security incidents are more prevalent in organizations. The incidents are more likely caused by insiders and they can happen with or without intentions. Although some security studies state that unintentional security incidents could cause more damages to organizational information systems (IS) than intentional security incidents, the research in this area is still limited. This paper focuses on unintentional employees' behaviors that have impacts on organizational information security, rather than unintentional behaviors in general IT practices. It explores unintentional information security behavior based on the perspective of the Qur'an and Hadith. Moreover, it provides some recommendations based on academic studies and Sharia teachings to overcome unintentional information security behavior. This paper starts with the discussion on information security behavior, human intentions based on the Sharia, and unintentional behavior under Islamic perspective. Finally, the significance of the study relies on the recommendation to reduce unintentional security threats based on information security studies and Sharia teachings by proposing a model to understand unintentional information security behavior and the factors that affect them.

***Keywords*:** information security behavior, unintentional security behavior, insider threat, Qur'an and Hadith perspective.

1. Introduction

Recently, it was reported that some organizations have been badly affected by information security breaches. These breaches have affected their reputation and cost them millions of dollars in term of financial damages. According to academic studies, the majority of information security breaches occur due to mistakes, negligence and carelessness of employees (Bulgurcu, Cavusoglu, & Benbasat, 2010; Herath & Rao, 2009; Safa et al., 2015; Warkentin & Willison, 2009). For example, an employee in Australia's immigration department has accidentally sent an email to an organizer of the Asian Cup soccer tournament that contains confidential information including passport and visa details of President Obama and 30 other world leaders who attended Group of 20 summit in Australia (Phillip, 2015). Another example was mentioned by Krebs (2015) in which an American organization exposed credit card data of their 25,000 customers. This incident happened when the hackers managed to access the company's information system (IS) by using the user name and password of a district manager who had his username and password attached to the front of his laptop.

Some security studies suggest that unintentional security behavior could pose more damages to IS than intentional security behavior (Abdul Molok, Ahmad, & Chang, 2010; Colwill, 2009; Fernando & Yukawa, 2013; Liu, Wang, & Camp, 2009; Loch, Carr, & Warkentin, 1992). Unintended security incidents can be easily repeated for employees' convenience and it is difficult to be detected by organizations until the damage has occured (Fernando & Yukawa, 2013; Guo, Yuan, Archer, & Connelly, 2011; Herath & Rao, 2009; Liu et al., 2009). In the same vein, Colwill (2009) mentioned that, these security incidents will continue to occur as long as the insiders have the legitimate access to the organizational IS.

It is estimated that more than half of IS incidents are directly or indirectly caused by inadvertent security behavior of the insiders (Colwill, 2009; Galvez, Shackman, & Guzman, 2015; Liu et al., 2009; Vance & Siponen, 2010; Walker, 2008). Although there are many studies which have already covered intentional threats and deviant insiders, studies that focus on unintentional behaviors are still limited (Crossler et al., 2013; Guo et al., 2011; Warkentin & Willison, 2009). Thus, this paper aims to study unintentional security behavior to answer the following questions:

1. What is the perspective of Sharia about unintentional security behavior?
2. What are the recommendations from the Qur'an and Hadith to overcome unintentional security behavior?

In conclusion, the answer to these questions may contribute to research and practicing in term of providing recommendations that can advance our understanding about unintentional information security threats. Consequently, organizations can understand different kind of insider threats and deal with them separately. As a result, that can increase the effectiveness in securing organizational IS and reduce the vulnerabilities to IS.

2. Research Background

2.1 Information Security

Information has become more valuable to organizations because they heavily rely on IS (Bulgurcu et al., 2010; Whitman & Mattord, 2011; Wybourne, Austin, & Palmer, 2009). In fact, any damage or threat to the information could affect organizations strategically, operationally and financially (Alhogail & Mirza, 2014; Crossler et al., 2013; Wybourne et al., 2009). Therefore, managing information security is taking high priority in many organizations (Bulgurcu et al., 2010). 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".

In line with the definition above, the effectiveness of information security in organizations depends on three components which are people, process and technology (Herath & Rao, 2009). However, most organizations often depend on purely technical-based solution to ensure information security (Bulgurcu et al., 2010; Fernando & Yukawa, 2013; Ifinedo, 2014). Technical mechanisms alone are not enough to keep organizations away from threats because information security is often the combination of "people issue", "technical issue" and "organizational issue" (Bulgurcu et al., 2010; Ifinedo, 2014; Workman, Bommer, & Straub, 2008). Thus, organizations need to have comprehensive approach that combines people, technology and process in order to protect their IS assets (AlHogail, 2015; Furnell & Thomson, 2009; Ifinedo, 2014). It is even preferred for organizations to focus more on humans because process and technical control mechanisms must suite the security behaviors of the employees (Bulgurcu et al., 2010; Fernando & Yukawa, 2013). It is stated that as long as employees have

full commitment to their management and the organizational security polices, organizations can achieve high level of information security and vice versa (Fernando & Yukawa, 2013; Ifinedo, 2014). For example, if one organization has a very advanced defense system while its end-users or insiders are behaving improperly (e.g., trying to breach the system or violating the policies and procedures), defense system would fail to achieve the organization's aim to protect their IS. In this paper, we agree with Herath & Rao (2009) that although many security controls can be automated by the technical control mechanisms, some employees' behaviors cannot be controlled by these mechanisms and therefore requires other means of controls such as security policies and education.

2.2 Insider Threats to Information Security

The trend of information security studies is now moving towards studying insider behavior and its impact on IS (Crossler et al., 2013; Kreicberga, 2010; Warkentin & Willison, 2009). In accordance to security studies the term of insiders is used to describe anyone who has legitimate access to IS and networks in the organizations (Colwill, 2009; Liu et al., 2009; Predd, Pfleeger, Hunker, & Bulford, 2008). They could be employees, auditors, outsourced employees or third party personnel, ex-employees, temporary business partners and more. In fact, insiders are the weakest link in the information security chain as they are naturally prone to make mistakes and have misunderstanding (Crossler et al., 2013; Fernando & Yukawa, 2013; Wybourne et al., 2009). Moreover, they are easily motivated and affected by their peers and the environment so their actions towards the IS can be unpredictable (Fernando & Yukawa, 2013; Hu, Xu, Dinev, & Ling, 2011).

Leach (2003) and Walker (2008) have argued that, threats to IS are usually result from poor security behavior of the insiders. Colwill (2009) also agrees that insiders have more advantages and the potential to cause harm more than outsiders because they have full access to IS. Furthermore, they know many things about the organization and its valuable assets that outsiders know nothing or little about (Colwill, 2009). Moreover, insiders can target the information directly without facing the barriers that are faced by the external hackers while outsiders need to collect huge data and information before they can attack the corporate systems (Colwill, 2009; Guo et al., 2011; Warkentin & Willison, 2009). They also need to have intelligent tools and spend long time in order to breach the security perimeter and access to the system. However, insiders can do that with almost zero efforts and time.

Nowadays, organizations have started to realize the insiders' impacts on their IS and the importance of managing insider threats. Recent report by Poll (2015) indicated that 89% of respondents (senior business managers and IT professionals) felt that their organizations were at risk from an insider attack and 34% felt extremely vulnerable by insiders. Furthermore, many organizations recognize the importance of their employees in protecting and strengthening the information security when employees comply with their information security rules and policies. Thus, organizations are shifting the focus of information security from "technology oriented" to "management oriented" and from "outsiders" towards "insiders" (Bulgurcu et al., 2010; Fernando & Yukawa, 2013).

According to Crossler et al., (2013) & Liu et al., (2009), insider security threats can be done with and without intentions. Although there are many studies about insider threats, most of them did not attempt to differentiate between intentional and unintentional violations of IS security (Alhogail & Mirza, 2014; Crossler et al., 2013). Accordingly, Crossler et al. (2013) stated that the mixing between intentional and unintentional security behavior can reduce the applicability and effectiveness of IS security measures. Many security studies agree that having

a comprehensive framework of insider behavior and their possible threats to IS, either intentionally or unintentionally, will effectively reduce these threats and thus may better protect organizational IS (Crossler et al., 2013; Fernando & Yukawa, 2013; Hu et al., 2011; Ifinedo, 2014; Predd et al., 2008; Safa et al., 2015; Warkentin & Willison, 2009).

2.3 Information Security Behavior

This section presents a review of literature that is related to intentional and unintentional information security behavior.

2.3.1 Intentional Information Security Behavior

This paper defines malicious insider as:

"A current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems" NCCIC (2014, p. 1).

Insiders are usually trusted and they have full access to the organizational IS. They 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). Malicious insider attacks are mostly planned and they target particular areas in IS. The targeted information could be trade secrets, intellectual property, top secrets, property information and users' information (Predd et al., 2008; Wybourne et al., 2009).

Colwill (2009) mentions that motivation, opportunity and capability are usually the main factors of any insider attacks. Therefore, organizations should understand these factors in order to prevent any potential threats. There are many motivations for insiders to engage in malicious behaviors. Some do it for personal gain, financial gain, their ego, their friends and others do it because they have the ability to do it (Liu et al., 2009). Motivations usually come from internal while opportunity and capability are given by organizations. This means that organizations with clear policies and healthy work environment may be able to manage and mitigate malicious insider risks (Colwill, 2009).

2.3.2 Unintentional Information Security Behavior

Those who breach IS without any intentions to harm are called inadvertent insiders and they are defined by Liu et al. (2009, p. 1) as:

"Trusted insiders who do not have malicious intent (as with malicious insiders) but do not responsibly managing security, and the results are often enabling a malicious outsider to use the privileges of the inattentive insider to implement an insider attack".

Despite huge coverage of intentional insiders threats and deviant security behavior, studies that focus on unintentional security behavior are still limited (Crossler et al., 2013; Guo et al., 2011; Warkentin & Willison, 2009). According to security studies, security incidents that are caused by insiders are more likely to be unintentional than intentional (Abdul Molok et al., 2010; Colwill, 2009; Fernando & Yukawa, 2013; Liu et al., 2009; Loch et al., 1992). They also posit that most of information leakage incidents and other security breaches are resulted from

accidental security behavior and human mistakes that could cause more damage to organizational IS (Abdul Molok et al., 2010; Colwill, 2009; Fernando & Yukawa, 2013).

Some scholars of information security argue that unintentional security incidents can be easily repeated for employees' convenience and it is difficult to be detected by organizations until the damage has been done (Fernando & Yukawa, 2013; Guo et al., 2011; Herath & Rao, 2009; Liu et al., 2009). Accordingly, it is estimated that more than half of IS incidents are directly or indirectly caused by inadvertent insiders (Colwill, 2009; Liu et al., 2009; Vance & Siponen, 2010; Walker, 2008). Hence, it is very important for organizations to be aware of unintentional security threats in order to prevent any possible threats that can be unintentionally posed by their employees.

Example of unintentional security behavior are selecting a simple password, visiting non-work related websites, unintentionally posting confidential data onto unsecured platforms such social networking sites, or carelessly clicking on phishing links on emails and websites (Crossler et al., 2013; Safa et al., 2015). From these examples we can see that employees might not have the intention to cause harm to IS. However, these actions are leading to information security breaches and those negligent insiders are responsible of their actions.

3. Human Intentions Based on the Sharia

As mentioned earlier, although there are number of studies about insider threats to information security, most of them did not attempt to differentiate between those who are intentionally or unintentionally violate the security of IS (Alhogail & Mirza, 2014; Crossler et al., 2013). In fact, popular Western theories on human behavior do not cover unintentional behavior. They often point intentions that lead to certain behaviors such as Theory of Planned Behavior (Ajzen, 1985), Theory of Reasoned Action (Sheppard, Hartwick, & Warshaw, 1988), and Protection Motivation Theory (Boer & Seydel, 1996). On the other hand, Islam has clearly distinguished between intentional and unintentional actions and behavior because each behavior or action in Islam is considered valid or void depending on human's intention (*niyyah*). Hence, the Qur'an and Hadith state clearly the rules and regulations to control intentional and unintentional actions and behaviors. For example, if a person intended to do good without doing it, he/she will be rewarded as prophet Mohammed peace be upon him (*pbuh*) said in Hadith narrated by 'Umar bin Al-Khattab: "*The rewards of deeds depend upon the intentions and every person will get the reward according to what he has intended*" (Sahih AL-Bukhari, Book 1, Hadith Number 1). Therefore, it is an obligation for Muslims to make a good and proper intention for every deed. Accordingly, any improper action that can result in harming other people or properties should be avoided. Based on that, employees should avoid any mistakes or improper actions which can lead in breaching the security of IS.

4. Unintentional Behavior under Islamic Perspective

The word "Human" in Arabic is known as "*An-Naas*" which is derived from the word "*nasiya*" which means forgetful (Adams, 2006). Hence, we indicate that the nature of human tend to forget and make mistakes (Adams, 2006). Consequently, Muslims should be aware of their actions to avoid mistakes and misbehavior. Muslims should always ask Allah to forgive their mistakes and forgetfulness as Allah says: "*Our Lord, do not impose blame upon us if we have forgotten or erred*" (Qur'an 2:286). Ibn Abbas said that "*Al-Insan*" is called so because of his forgetfulness and he derived that from Qur'an when Allah says about Adam: "*And We had already taken a promise from Adam before, but he forgot*" (Qur'an 20:115). In general, unintentional behavior and human mistakes might be pardoned by Allah as He says in Surah Al-Ahzab: "*But there is no blame on you if you make a mistake therein: What counts is the*

intention of your hearts" (Qur'an 33:5). Ibn Abbas reported that the Messenger of Allah (*pbuh*), said: "*Truly Allah has for my sake pardoned the mistakes and forgetfulness of my community, and for what they have done under force or duress*." A fine hadith related by (Al-Baihaqi, Al-Sunan book, Hadith number 7 &, Ibn Majah, Hadith number 2045). However, if these unintentional actions or mistakes have caused harm to other people or properties, the offender must take full responsibility to fix all damages that he caused. In line with the Hadith narrated by Anas: "*One of the wives of the Prophet (pbuh) gave the Prophet (pbuh) some food in a bowl. Then 'Aishah broke the bowl with her hand, and discarded what was in it. So the Prophet (pbuh) said: "Food for food and vessel for vessel*" (Jami` at-Tirmidhi, Book 13, Hadith number 1359).

Reflecting the above verses from the Qur'an and Hadith to the information security behavior, we can learn that, employees are requested to follow the guidance and the policies which are provided by their organizations for best practices in information security. Messenger of Allah (*pbuh*) said: "*The Muslims will be held to their conditions, except the conditions that make the lawful unlawful, or the unlawful lawful*" (Jami` at-Tirmidhi, Book 13, Hadith number 1352). Therefore, employees are held to their agreement with their organizations in which they are requested to comply with their information security policies and procedures in order to protect organizational IS. Hence, anyone breaks the information security rules and polices, the organization has the right to punish him.

The employees are trusted people in most of organizations and they are given full access to IS to perform their work. Moreover, the employees in most of organizations are requested to fulfil their responsibility towards keeping the information confidential and not revealed to unauthorized individuals. Allah says in the first verse of *Surat Al-Mā'idah*: "*O you who have believed, fulfil [all] contracts*" (Qur'an 5:1). Therefore, employees should be aware of their information security behavior by avoiding carelessness or negligence that can lead to breach organizational IS. Allah's Messenger (*pbuh*) said, "*All of you are guardians and are responsible for your subjects*" (Al-Bukhaari and Muslim, Book 1, Hadith number 300).

On the other hand, organizations also have very important part and big responsibility towards their employees. Organizations are supposed to provide information security training and education programs to spread awareness to their employees. Additionally, they should have clear policies that show the permitted and prohibited actions and the sanctions in case of any breach either with or without intentions.

As mentioned above, unintentional security behavior can be easily repeated for employees' convenience and it may occur many times in different cases by the same employee or others. Nevertheless, Prophet Mohammed (*pbuh*) 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). The meaning of this Hadith is that Muslims should be aware of their actions and should avoid repeating the same mistakes twice.

5. How to Overcome Unintentional Security Behavior

Organizations will continue to suffer from unintentional security behavior unless they provide a comprehensive solution to be followed. In fact, the main focus of any organization should be the insiders or employees as mentioned above since they are the weakest link of information security chain. It also confirmed in the Qur'an that humans are created weak when Allah says: "*And mankind was created weak*" (Qur'an 4:28). Therefore, organizations have to understand

the employees' need and provide them with a security conducive environment so that they have time to complete their work tasks while observing information security practices.
It is widely suggested for organizations to implement and develop plans, policies and governance structures to encourage the compliance with security policies and procedures (Crossler et al., 2013; Herath & Rao, 2009; Ifinedo, 2014; Siponen, Pahnila, & Mahmood, 2010; Warkentin & Willison, 2009). By doing so, employees will have the knowledge of the best security practices while using the IS.

The top management is responsible to continuously remind their staff and update them from time to time about security vulnerabilities to IS and expose them to some current and real cases of security breaches. Moreover, they are also responsible to provide proper knowledge and guidance about information security misbehavior in order to remind their staff of their responsibility in protecting the organizational IS. In similarity to that and based on Islamic perspective, Allah says: "*And remind, for indeed, the reminder benefits the believers*" [Noble Qur'an 51:55]. Allah's Messenger said, "*The deen (religion) is naseehah (advice, sincerity)." We said, "To whom?" He said, "To Allah, His Book, His Messenger, and to the leaders of the Muslims and their common folk*" (Muslim, 40 Hadith Nawawi book, Hadith Number 7).

Abdul Molok et al., (2010) recommend information security education, training and awareness (SETA) programs to be implemented in the organizations. As a result, organizations will make sure that employees understand their organizational policies and their responsibilities towards information security. Employees also should share the advice and knowledge of how to protect IS, warn those who are behaving improperly and report them to the top management if their actions would jeopardize organizational information security. What is more, senior employees should guide others to the best security behavior if they found others behaving improperly. Prophet Mohammed (*pbuh*) said, "A *believer is the mirror of his brother. When he sees a fault in it, he should correct it*" (Al-Albani, Al-Adab Al-Mufrad Book, Hadith Number 238). Moreover, Muslims can recite some prayers (*Doa'a*) that are mentioned in Qur'an and Sunnah to avoid falling in unintentional or improper behavior. One of these prayers that is mentioned by the Messenger of Allah to be recited while leaving home, Umm Salamah reported: Whenever the Prophet (*pbuh*) stepped out of his house, he would say, "*I begin with the Name of Allah, I trust in Allah; O Allah, I seek refuge with You from going astray or stumbling, from wronging others or being wronged, and from behaving or being treated in an ignorant manner*" (Sunan Ibn Majah, Book 34, Hadith number 3884).

To summarize our proposed recommendation to overcome information security incidents, this paper presents a conceptual model as illustrated in Figure 1. This model explains the countermeasures of unintentional security misbehavior based on Islamic perspectives and information security studies. It shows the importance of three elements namely individuals, peers and organization or top management in protecting IS and enhancing information security. The model depicts the roles of individuals to make *doa'a*, to comply with organizational policies and procedures, and to have a sense of responsibility in order to guide their intentions which will lead to the information security behavior. It also highlights the duty of peers to provide advice and help, and be responsible to report any violations to security policies to the management. Additionally, the model portrays the roles of the organization to enhance information security by developing and implementing security policies, employing technical control mechanisms and providing SETA to their employees.

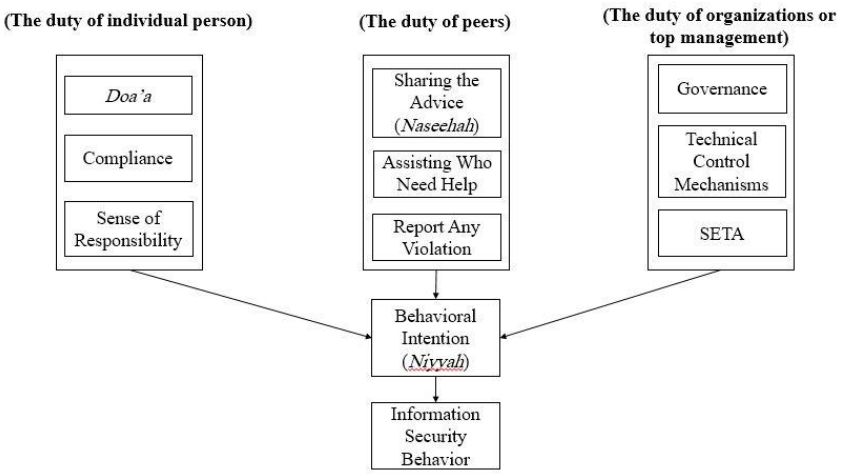

Figure 1. Countermeasures of Unintentional Security Behavior

6. Conclusion

Although organizations have started to realize the impact of unintentional security behavior to their IS, yet this issue has not been covered widely in academic studies and empirical research. For future research, we suggest more studies on a comprehensive framework that covers all security behavior whether it is intended or not intended, malicious or non-malicious, intended (non)malicious and unintended (non)malicious types of security behavior. Consequently, with the ability to distinguish these kinds of security behaviors, organizations will have effective solutions to different kinds of security threats. Based on literature review, this conceptual paper explores unintentional security behavior from the Qur'an and Hadith's perspective and relate them with Western theories to provide the proposed solutions and recommendations for organizations and Muslim Ummah at large in order to overcome unintentional security behavior within the organizational IS.

References

Abdul Molok, N. N. A., Ahmad, A., & Chang, S. (2010). Understanding the factors of information leakage through online social networking to safeguard organizational information. In ACIS 2010 Proceedings - 21st Australasian Conference on Information Systems. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84870387706&partnerID=tZOtx3y1

Adams, D. (2006). The Five Pillars of Islam. Retrieved from http://h2g2.com/edited_entry/A4114009

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. Springer, 11–39.

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. http://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. http://doi.org/10.1016/j.chb.2015.03.054

Boer, H., & Seydel, E. R. (1996). Protection motivation theory. Predicting Health Behavior. http://doi.org/10.1080/13548506.2011.579983

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.

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. http://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. http://doi.org/10.1016/j.cose.2012.09.010

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. http://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.

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. http://doi.org/10.2753/MIS0742-1222280208

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. http://doi.org/10.1016/j.dss.2009.02.005

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? Communications of the ACM, 54(6), 54. http://doi.org/10.1145/1953122.1953142

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. http://doi.org/10.1016/j.im.2013.10.001

Krebs, B. (2015). Deconstructing the 2014 Sally Beauty Breach. Retrieved from http://krebsonsecurity.com/2015/05/deconstructing-the-2014-sally-beauty-breach/#more-30872

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

Leach, J. (2003). Improving User Security Behaviour. John Leach Information Security Limited, (September).

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. http://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.

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

Phillip, A. (2015). Australian official accidentally e-mailed out the number. Retrieved from http://www.washingtonpost.com/news/morning-mix/wp/2015/03/30/australian-official-accidentally-released-passport-info-for-obama-30-other-world-leaders-report-says/

Poll, H. (2015). VORMETRIC INSIDER Trends and Future Directions in Data Security.

Predd, J., Pfleeger, S. L., Hunker, J., & Bulford, C. (2008). Insiders behaving badly. IEEE

Security and Privacy, 6(4), 66–70. http://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. http://doi.org/10.1016/j.cose.2015.05.012

Sheppard, B., Hartwick, J., & Warshaw, P. (1988). The Theory of Reasoned Action: A Meta-Analysis of Past Research with Recommendations for Modifications and Future Research. Journal of Consumer Research, 15, 325–343.

Siponen, M. T., Pahnila, S., & Mahmood, M. A. (2010). Compliance with Information Security Policies : An Empirical Investigation. IEEE Computer Society, 64–71. http://doi.org/10.1109/MC.2010.35

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

Walker, T. (2008). Practical management of malicious insider threat - An enterprise CSIRT perspective. Information Security Technical Report, 13(4), 225–234. http://doi.org/10.1016/j.istr.2008.10.013

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

Whitman, M., & Mattord, H. (2011). Principles of Information Security. Learning. http://doi.org/10.1016/B978-0-12-381972-7.00002-6

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

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24(6), 2799–2816. http://doi.org/10.1016/j.chb.2008.04.005

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