INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES
HRMARS MANAGEMENT ACADEMIC RESEARCH SOCIETY EXPLORING INTELLECTUAL CAPITAL
www.hrmars.com
ISSN: 2222-6990

Information Security Behaviors among Employees

Nor Natasha Ashira Shamsudin, Saiful Farik Mat Yatin, Nurul Fadhlin Mohd Nazim, Amie Witiza Talib, Mohammad Afiq Mohamed Sopiee, Fifi Natasya Shaari

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v9-i6/5972 DOI: 10.6007/IJARBSS/v9-i6/5972

Received: *10 April 2019,* ***Revised:*** *19 May 2019,* ***Accepted:*** *03 June 2019*

Published Online: 29 June 2019

In-Text Citation: (Shamsudin et al., 2019)

To Cite this Article: Shamsudin, N. N. A., Yatin, S. F. M., Nazim, N. F. M., Talib, A. W., Sopiee, M. A. M., & Shaari, F. N. (2019). Information Security Behaviors among Employees. *International Journal of Academic Research in Business and Social Sciences*, *9*(6), 560–571.

Vol. 9, No. 6, 2019, Pg. 560 - 571

http://hrmars.com/index.php/pages/detail/IJARBSS | **JOURNAL HOMEPAGE**

INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES
www.hrmars.com
ISSN: 2222-6990

Information Security Behaviors among Employees

[1]Nor Natasha Ashira Shamsudin, [1,2]Saiful Farik Mat Yatin, [1]Nurul Fadhlin Mohd Nazim, [1]Amie Witiza Talib, [1]Mohammad Afiq Mohamed Sopiee, [1]Fifi Natasya Shaari

[1]Faculty of Information Management, Universiti Teknologi MARA (UiTM) Selangor, Malaysia
[2]Members of Advanced Analytics Engineering Center (AAEC), UiTM
Email: farik@salam.uitm.edu.my

Abstract

Information Security is crucial to organization especially to financial and industrial when dealing with company information and data. Information Security is defined as protecting the information and information system from unauthorized access, use, disruption, modification, disclosure, or also the destruction which to provide the confidentiality, availability, and integrity of the information. Information Security role as protecting the information and systems that covers compliance which involves data protection and publication scheme, and Information Management for Corporate Records, Copyrights and Intellectual Property. In this fast-changing world today, mobile technologies in information age nowadays have the ability and advance functions of computers and connectivity. In everyone's daily life, technologies have become integral and ubiquitous without their realization and user is vulnerable to the cyber-attack. Criminal hackers are attracted to steal personal and organization information. Thus, corporate data must be prevented from being transferred to personal application whether it is on personal devices or computer networks. As for organization, information and data are crucial for their organization plan, business conducts and future successfulness. This article will discuss issues, awareness, types of behavior, compliance and policies regarding information security.

Keywords: Information Security, Information Age, Security Behaviors, Information Organization, Information Management

Introduction

Information security can be defined as data protection from threats or risk either for organization or individual. According to Hall, Sarkani and Mazzuchi, (2011) the rapid changes in today's global of advancing information technologies have driven the great challenges to the information security which makes people facing more risk when dealing with technologies such as computers, mobile devices, smart phones and etc. In today information age with the new technologies, many things can be done with this technology as an example, online banking use various applications and social networking sites, shop online, share locations, and other personal details. These activities attract criminal hackers to steal user's personal information. Security issue such as viruses, worms, malicious software and much more threats might cost big lost in organization such as security and physical threats in business continuities, environmental hazards, and malicious attacks in cyber threats, espionage, and denial of service (DoS) (Abraham, 2011). The valuable assets should be protected appropriately in order to ensure safety of the information; every organization needs to apply security measures in which controls systems and operations internally, and also protecting the integrity and data confidentiality.

Furthermore, to have great security implementation, users or employees in organizations must comply with securing the information. Every users must know how to protect the information them self by adjusting their security setting and choose the best application. Understanding on the risk and also prevention might help reducing the risk of cyber threats and data loss. Security is all about preventing all sorts of threats from the intentional and unwarranted actions. The objective of information security is to build protection against criminal actions intentionally. Management and IT management are responsible for implementing information security in their organization while personal safety awareness might help protecting personal self-security.

Confidential information can be considered as organization assets that turn into competitive advantages for make them better than opponent or others. It is either in business-oriented company or vice versa, by segmenting the data and available information is not the only criteria, but by using it accurately for operations to help grow their corporation in a very efficient way. Malaysia have experience the biggest mobile data breach on October 2017 where 46.2 million number were leaked online is reported including transferring funds into their bank accounts, and installing TELCO applications containing Malware for the next exploitation. Generally, no system is unhackable even in the US Department Defense but some precaution must be done as a taking step to restrict it from occurs repeatedly.

Issues with Information Security among Employees in Organizations

Threat might occur from the external and also internal aspects. Threat brings affect in a sort manner which can bring downfall of the organizations. Security threats and attacks can lead to the degrading in term of performance and productivity within the organization such as threats that came from externally aspects or known as external threat that can be related to an outsider that breaches the information security of the organization. Meanwhile, threats that came from internal aspect can relate to managerial itself and staffing.

Internal Threats

One of the issues identified is threats to information or assets of the organization from employees. The highlight is more on the employees or the staffs itself within organizations. Li (2015) stated that the greatest concerns in organizations to the information systems security managers is when the information security threats and attacks come from insiders or specifically known as workers or employees within the organizations. Therefore, the role of information security is to protect the information and ensuring the confidentiality and integrity of information, including maintaining its availability. Information security apparently impact on the management within the organizations as the effective security management to ensure the success of business operations.

However, people within or employees are seen as critical factors towards the protecting and securing the information and there is always complexity between them and technical elements which their role in the information security management implementation should not be ignored within organizations.

Employees with high morale of information security will tend to look upon their information or asset seriously. High morale of awareness will ensure the safe-keeping of valuable within the holding. Other than that, the information security risks related to human activities have been observed among employees from large and medium size of business which employees are violating company and organization security policies or else personally engage with the security thefts. Management in organizations are starting to focus on the employees and staff's behaviors towards information security as the claim made by Pattinson et. al., (2016) that the biggest security issue is still linking between the keyboards and the chairs which addressing the behaviors of computer users.

Employees in organizations do not comply with organizational rules and regulations of information security. Employee that acts seldom in performing job related tasks can affect the security of information. The employment of employee or recruitment will always involve the briefing of rules and regulations of those particular organizations. Employees are already exposed with the rules and regulations upon given acceptance. Many staffs do not take that rules and regulations seriously and always try to skip the necessary procedures as it is too formal and will find the easiest ways in performing their jobs. This ignorance can affect the designated procedures as the rules and regulations are done purposely. Lack of sense in performing their jobs based on the rules of organization will create an open door for any attackers and mistakes that might happen to the asset of organizations.

As in the external factors that influence the information security behaviors among people in the organizations, Hacking issues is one of the cyber threats that is emerge in today era through the connectivity of internet. The capabilities of internet connectivity lead to many security threats to users (Jones and Chin, 2015; Kraus et al., 2017). Internet can be useful in performing multiple transactions or operations within the organization. This benefit can help the organization in doing task such as virtual conferences, undergoing bank transactions, blasting meeting notifications to committee, transferring of data remotely and other benefits. It is indeed, the existence of internet connectivity can help various organizations in performing their daily operations. But by having these

facilities, there are certain entities that will try to lurk into the organization holdings which is referring to their data. The intention of these entities is no order to steal vital information or making deterioration within the targeted organizations. These entities are referred to the hackers.

There are hackers that doing this underground activity by their own, in groups and even might be hired from the competitors within the nature of business. The jealousy of achievements of competitors can lead to the hiring of hackers in making an issue within the targeted organizations. These hacking activities come with a price. The higher the values of targeted information by the hackers can lead to potential big loss towards organization.

The issues that need to be highlighted here is regarding to privacy concern of information. There is lots of crucial information within the organization such as clients' information, banking accounts, policies data and so on which can affect the confidentiality, integrity and availability of information once there is breaching to the information. Upon hacking have been successfully done, the contained data within the organization might be altered or loss, this lead to the unable to perform certain transactions such as purchasing of materials or liaising with the vendors. It is in fact, the strengthening of firewall within the network of organization needs to be look upon by every organizational management as these hackers will breach the security within connectivity of internet which is relating to network aspect. The availability of Wi-Fi connectivity need to be taken seriously as this is one of the platform for hackers in accessing the network within organization. For example, if there are staffs that perform remote assignment far from the organization, they need to connect to secure internet connectivity as their devices such as laptop and Smartphone devices might contain organization's data that is targeted by this hacker.

Theoharidou et al., (2012) stated that there are many different types of data that might be stored within their Smartphone that may include personal, business, financial, government, and authentication as well as connection data. The use of free Wi-Fi need to be avoided as possible as it is not preferred to be used for working purposes in term of security. Unsecured or unknown access point can bring harmful for Smartphone user because wireless connectivity operating by transmitting through the air and expose to external threat than wired connectivity (Sharma and Gupta, 2016). The use of Virtual Private Network (VPN) is crucial in such case there is no secure connectivity available within range.

Apart from that, the malware attack issues also the factor that influences the information security behavior among employees in the organizations. Malware or also known as malicious software is available over the internet and can be spread to various methods such as downloading unknown attachment sources, universal serial bus infections, surfing harmful internet sites and many more. This unwanted software is no use in term of functionality within a computer. Only harm can this malicious software brought to user such as consume a lot of space with junk files, installing advertisement within the storage, installing additional software without user consent, deleting existing files within computer, duplication of files and so on. Various example of malware are adware, bots, bugs, rootkits, spyware, Trojan horses, viruses and worms. According to Roman, (2017) by

referring to Kaspersky lab report, it was detected around 8.5 million malicious software installation, over 128, 886 mobile banking Trojans, and 261, 214 mobile ransom ware Trojans. This shows that malware attack can occur from several of forms and methods in which this can breach the security of information and brings effect to the organization holdings. Malware is created by unethical entities in order for them to steal data, brings alteration to files which breaching the authority of the files and other harmful behaviors. It is necessary for every organization to perform backup once in a while in order for them to have safety precautions in term of vital information that contained within organization repositories.

Kim, (2013) stated windows operating system provide actions center which functioning as alerts for user to performs backups. Performing backups and being aware of security alerts notification needs to be highlighted when operating any business upon the computer used in daily operation.

Information Security Awareness among Employees with Technological Changes

Every data and information that managed by staffs is considered as valuable assets to the organizations. The attitudes upon managing the information at the workplaces must be look upon seriously by the managerial as there are staffs with high motivation of work will performs efficiently and there will be some of the staffs that have low motivations. Employees that have low motivation will tend to work in efficient and slow progressive as this must be look upon their attitudes at the workstations. Every aspects on their log in, log off when using computer must be taken seriously as the assigned staff is given responsibility in managing the information. Every employee within the organization is given special ID which is only authorized to be used by them only. The lack of awareness of log off from their accounts can lead to the leak of information to unauthorized entities. Any attacks from cyber space might occur when necessary measures are not well-managed. Further elaboration is on advancement of technologies leading to newer cyber-attack.

Information security is seen as challenges in organizations and companies because the massive advancement and development of information technology sector has increased the technological needs in organizations and among its people within. As mentioned by Stewart and Jurjens, (2017) in their research that these security issues occur among people especially in the organizations because of various factors that lead to the threats to a company's information security which is the poor information security awareness among employees, training, and managed teams. As stated in the report there are about 58 percent of the cyber security incidents occur in the public sector which were caused by the employees, incidents in handling the data, and malicious data used by the employees within the organization. Hence, this recognized that human behaviors are the weakest link in protecting the personal and sensitive information when it comes to information security. The individual users are the critical for ensuring the information security in this Information Age. The existing technologies are still facing cyber-attack by time to time. Attackers will always find new methods in breaching the firewall of organization for no good purposes. Organization should always keep update on the lasts security credential in ensuring their data safe from any possible cyber-attack that could happen. They should always check their current firewall either it is safe to perform any online transaction without having any hackers that might be stealing their information.

Once the data is placed on the wrong hand or in this aspect the attackers, the valuable information might be sell to other third party for the sake of money. Once the data is placed on the wrong hand or in this aspect the attackers, the valuable information might be sell to other third party for the sake of money. This will lead to the leak of information to organization's competitors as well as poor managerial in term of defense from cyber-attack. The avoidance of performing job related without security compliance can affect the overall performance when things are out of hand. Lack of awareness on the level of secrecy of document should be avoided by employee in avoiding unnecessary leakage.

Types of Information Security Behaviors in Organizations

There are three (3) types of behaviors of people in organizations towards the information security which are deliberate risk averse, deliberate risk inclined, and naive and incidental behaviors Pattinson et al., (2016).

Naive and Accidental Behaviors

Specifically, explains that the attitudes of the computer users which is employees in the organizations. They leave the computer unattended, use the social networking sites, open spontaneous email attachments, apply guessable password that easier for people to hack into, no reports when there are security incidents, and get access into suspicious websites.

Deliberate Risk Averse Behaviors

The deliberate risk averse behaviors are the type of behavior when people in organization are aware with the information security deployment in protecting the information and privacy such as always log off when the computers and desks, always make reports for any security threats and accidents, regularly change password, install antivirus, and block for spams.

Deliberate Risk Inclined Behavior

The other type is deliberate risk inclined behavior in which this type of behavior that intended to perform crimes and security threats to people organizations that can cause many security issues and threats such as hack into people's accounts and personal access, conduct crimes and information security attacks, create spam emails, and give unauthorized access to unauthorized zones. Employees' behaviors are the most common obstacle associated with information security compliance. Employee behavior is relating to actions taken upon performing job related task. A good attitude and morale will lead to better behavior while as poor behavior will lead inefficiency of work. Every single task related that involve the handling of data must be taken with security compliance. This is related to not exposing data to unauthorized person, secrecy of information, security measures in transferring information and so on.

Table 1: Types and examples of information security behaviors among employees in organizations.

Types of Behaviors	Example of behaviors
Deliberate risk averse behaviors This type of behavior is people that are aware with the information security deployment in protecting the information and privacy.	1. Always log off when leave the computers and desks. 2. Regularly change for password Install antivirus, firewall and software update. 3. Vigilant in detecting the unauthorized access. 4. Always perform back up for works make reports for any security threats and incidents. 5. Block for spam, and disallow email, attachments, and phishing from unknown.
Deliberate risk inclined behaviors Type of behavior that intended to perform crimes and security threats to people and organizations that can cause many security issues and threats.	1. Install and use unauthorized software for company or personal computers, create and send for spam emails. 2. Hack into other people's accounts and personal access and known as theft for hardware and software. 3. Conducting crimes and information security attacks activities, give unauthorized access to an unauthorized zone. 4. Install and execute games or applications on the company or personal computers.

Naive and accidental behaviors This type of behavior is opposite from deliberate risk averse behaviors that are likely to get attack and threats from information security.	1. Leave the computer without log off unattended. 2. Open and access into spams and unsolicited emails, and access into unsafe or secure websites. 3. No antivirus installed and updated software. 4. Not being aware for any unauthorized access or information attacks and no reports for any security incidents occurred. 5. Easily share for ID and Password.

Information is an asset that provides valuable meanings for organizations towards effective decision making and in return giving the profit to the organization. However, protecting the valuable information which are assets for companies and organizations should be taken seriously as the advancement of technologies, social media, and Internet of Things (IoT) in today's Information Age provide not only many opportunities and advantages of information sharing, but also challenges that includes the information security and privacy risks (Alshare, Lane and Lane, 2018).

Reluctant to Comply Information Security in Organizations

Information security on the technical level in some organization and institutions such as bank and automobile were still using legacy technology devices and traditional information security management standards that do not meet their needs. Every once in a while, organization should keep their information security adaptation updated and coherence with the current generation in ensuring the security is well-managed. This is referring to the update of technologies and procedures that is aligned with digital age. In ensuring the information security always in the best state, managerial level should perform a survey on the latest news regarding to information security.

In order to sustain in the market, latest technologies are necessary as update can help to strengthen the defense from cyber-attack as well as providing efficient data management. Allocation budget must be assigned for the update that will be made as it involves costing. In the organizations, employees were reluctant to share knowledge or collaborate in the context of information security. Every employee within organization is responsible in implementing information security awareness

within working station. They should have the responsibility to always update on the latest knowledge on information security.

Reminding others on the information security is a must within working environment so that they know do and do not upon managing information. The reluctant of sharing knowledge or collaborating in information security should be avoided for the sake of safe-keeping the asset as all of the employees are responsible to the effect on the asset of the organizations. They should avoid their ego in term sharing knowledge on information security as someone might get penalty for their reluctant and it is not a healthy environment.

Apparently, this describes the employees' responsibilities towards the information use and access in the organization and the distribution of information that are confidential for organizational use. According to Yazdanmehr and Wang (2016) confidentiality means to protect the information from unauthorized access by making sure that information shared among are only among authorized users who have access.

Information Security Policies (ISP) in Organizations

Alshare, Lane and Lane, (2018) mentioned in the study that organizations have a tendency to make the data security strategies (ISP) to lessen and encourage the practices which are unacceptable for assortment of reasons such as proprietary access to information, avoidance from the outer entrance of the framework in managing productivity of employees applying the policies, restrict access to the external sources, and ranging from the information security. The right method is the key to effective information security. Many organizations often take the strategy of basically going down a checklist, check off prerequisites, and not putting excessively thought into the risks that the organization faces.

Information Security managers recently endorses to the organizations to utilize and implement general data security for coordinating and facilitating people, process, and technology towards the effective defenses across the organizations in order to avoid the malicious assaults and security threats from inside or outside the organizations. Numerous internet-enabled devices come with a set of default qualifications hard-coded inside. Such credentials are usually freely accessible on the web and widely known to offenders.

Moreover, managers have to emphasize the harshness and speed of penalty for any infringement of information security measures by setting up restrictive rules and practicing the disciplinary actions in a convenient way. This would be reliability of supportive organizational security culture.

A written policy serves as a centralized, formal guide to all best practices for information security as well as all security measures utilized as a part of the organization. It also allows them to make sure that their security specialists and employees are in agreement and give them an approach to authorize rules that protecting their data.

Other than that, a clear scheme will aware the employees of the consequences of their actions which could influence the employees' behaviors. Managers should make it clear to all employees that the authorizations for infringement of information security measures will be applied justifiably and with justice regardless of the status of the violator. All of these steps suggestion will have a stronger effect on employees' behaviors if they are supported by or encouraged with a company culture that nurtures information security minded thinking and considers information security to be a key standard.

With a specific end goal to make a culture that helps construct a feeling of network will help in making a positive environment in regards to sharing responsibility in ensuring organization's assets. This will include other factors that might be such impacts for employees' behaviors such as infringement writes, job responsibility, employees' affective commitment, rewards, fear, association composes, and culture.

Additional, the organizations or government sectors should give careful consideration in developing specific training programs to give and guide appropriate information security practices that could prompt the information security improvement. A much-improved arrangement is to utilize the rule of least privilege, in other words to appoint each new record the least privileges possible and to escalate privileges as necessary. At the same time, when access to delicate information is no longer needed, all corresponding privileges should be immediately revoked. The best approach to limit the risks of an insider assault by privileged users is to constrain their numbers.

Conclusion

The importance of information security should be emphasized in any organization culture and each of the employee. The impacts may not be seen in a blink of eye yet may lead to cause some chaos in that particular organization or the worst in the whole country as well. There are few standards available in the market that top management need to recognize and aware about it. Security compliance such as Information Security Policy (ISP) will enhance employee conduct in complying the policies. Failure to comply with the requirements such of Information Security guidelines may lead to disciplinary action. Employee should encourage and support by convene training course or information related to security awareness. The lack of adoption or depth understanding on how to implement related strategies is also found as one of the factors contribute to the poorly of management with respect to information security. Furthermore, the organizational capabilities also must be taken into consideration as factors such as sense making, asset availability and operation management can really contribute to the process of information security strategies to be implemented. All parties without any exception are involved in issues related to information security even from the government, higher level of management, respective organization, employee and employee regardless users at the end of the dissemination of information cycling process.

Acknowledgement

This paper was partially funded by:

1. Conference Support Fund, Institute of Graduate Studies (IPSis, UiTM)

2. Management Fund, Faculty of Information Management, UiTM

References

Abraham, S. (2011). Information security behavior: Factors and research directions. *17th Americas Conference on Information Systems 2011*, AMCIS 2011, 5, 4050–4062.

Alshare, K., Lane, P. L., & Lane, M. R. (2018). Information security policy compliance: a higher education case study. *Information and Computer Security*, 00–00. https://doi.org/10.1108/ICS-09-2016-0073

Hall, J. H., Sarkani, S., & Mazzuchi, T. A. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security*, 19(3), 155–176. https://doi.org/10.1108/09685221111153546

Jones, B. H., & Chin, A. G. (2015). On the efficacy of smartphone security: A critical analysis Of modifications in business students' practices over time. *International Journal of Information Management*, 561-571.

Kim, B. E. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security*, 115-126.

Kraus, L., Wechsung, I., & Moller, S. (2017). Psychological needs as motivators for security and privacy actions on smartphones. *Journal of Information Security and Applications*, 34-45.

Li, Y. (2015). *Users' information systems (IS) security behavior in different contexts*.

Pattinson, M., Parsons, K., Butavicius, M., McCormac, A., & Calic, D. (2016). Assessing information security attitudes: a comparison of two studies. Information and *Computer Security*, 24(2), 228–240. https://doi.org/10.1108/ICS-01-2016-0009

Roman, U. (2017). Mobile malware evolution 2016. Retrieved from secure list: https://securelist.com/mobile-malware-evolution-2016/77681/

Stewart, H., & Jurjens, J. (2017). Information security management and the human aspect in organizations. *Information and Computer Security*, 25(5), 494–534. https://doi.org/10.1108/ICS-07-2016-0054

Sharma, K., & Gupta, B. (2016). Multi-layer Defense against Malware Attacks on Smartphone Wi-Fi Access Channel. *Procedia Computer Science*, 19-25.

Theoharidou, M., Mylonas, A., & Gritzalis, D. (2012). A Risk Assessment Method for Smartphones. *Information Security and Privacy Research,* 443-456.

Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, 92, 36–46. https://doi.org/10.1016/j.dss.2016.09.009

Corresponding Author: Saiful Farik Mat Yatin. Faculty of Information Management, Universiti Teknologi MARA (UiTM) Selangor, Malaysia