Computer and Information Science; Vol. 12, No. 2; 2019
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Safeguarding the Information Systems in an Organization through Different Technologies, Policies, and Actions

Hend K. Alkahtani[1]

[1] Princess Norah bint Abdurahman University, Saudi Arabia

Correspondence: Hend K. Alkahtani, Princess Norah bint Abdurahman University, Saudi Arabia. E-mail: hkalqahtani@pnu.edu.sa

Received: March 9, 2019 Accepted: April 1, 2019 Online Published: April 30, 2019

doi:10.5539/cis.v12n2117 URL: https://doi.org/10.5539/cis.v12n2p117

Abstract

Background: Information system use has substantially increased among the organization based on its effective integration of the resources and improved performance. The increasing reliance on the information system serves as a great security threat for the firms. Objective: The study intends to evaluate the security of the information system in the organization located in the region of Saudi Arabia, concerning the user's awareness level. Methods: The quantitative design of the study is adopted which uses the survey approach. A close-ended questionnaire is used for evaluating the awareness level among the individuals. A total of 109 participants (males and females) in the Saudi Company were recruited for the study. Results: Despite the implementation of the policy, employees were unaware of it. The study highlights that the development of the firm's information security policy requires the firm to make employees aware of the significance of the information security. Conclusion: The study concludes that the organization needs to educate the workforce of the information security policy and develop their necessary understanding of the information security system. This allows the employees to identify and report security threats and risks which helps in the improvement of information security awareness.

Keywords: information systems, information security, security awareness, saudi arabian culture, security policy

1. Introduction

Information and technology involve the collection, processing, and transferring of information. Data needs to be collected from within and outside the organization to complete the process of planning and control through the communication channel (Babaei & Beikzad, 2013). Accurate processing of information is important as it presents timely and necessary information for decision making. At times, organizations are disturbed as a result of unnecessary information leading to confusion and continuance of activities. Safa et al (2013) explained the technological aspects addressing information security; however, it does not guarantee a secure environment for information. The technological aspects covered by Safa et al (2013) included; anti-virus, anti-phishing, anti-malware, anti-spam, authentication, anti-spyware, firewall, and intrusion detection systems.

A breach is likely to be created by the hackers as they target people, rather than the computers. It is important to combine the behavior of information security and technological aspects as stated by Furnell and Clarke (2012). Therefore, the risk of information security breaches in the information security environment can be mitigated by applying security approaches. Recently, users are misled by new methods and applications like fake anti-virus scanning or bogus disk defragmentation. A study conducted by Kim et al (2015) stated that the misleading application being displayed on the computer screen usually report non-existent threats. The impact of these effects can be mitigated through knowledge sharing (2015).

There are no computerized information systems in the knowledge-intensive organizations including the universities of Middle Eastern countries and Saudi Arabia. In Saudi Arabia, the adoption of the internet was limited because of certain barriers such as language, culture, and religion. However, a new information system named Banner Information system was introduced in 2009 that comprised of a comprehensive information database system, containing information about students, faculty, staff, and courses (Doherty, Anastasakis & Fulford, 2009). It also consists of a number of modules such as admission, registration and graduate student information. However, majority of the organizations, specifically universities face significant issues in securing their information systems.

It is a challenging activity among knowledge-intensive organizations (universities) to guarantee the security of information systems (Doherty, Anastasakis & Fulford, 2009). Majority of the Saudi universities are facing specific

issues associated with people awareness, law, and culture after the recent shift to the electronic networked information system. This system may also be a threat to the information system security; although, it is considered as an asset to help in reducing risk to information leaking or breaching (Bulgurcu, Cavusoglu & Benbasat, 2010). A human error may even cause significant damage to the information system due to the lack of knowledge and experience of using a computer.

It is impossible to catch the accused when theft occurs due to a lack of physical security system in Saudi Arabia. The use of tunnels and other service area providers offer an ideal environment to move unobtrusively in the case of auxiliary staff. These universities need to take serious actions for deterring hackers and the theft of software in Saudi Arabia. Based on the law, Royal decree no. M/17 8 Rabi 1 1428 / 26 March 2007, cyber-crimes are combated by identifying crimes to ensure enhancement of information security and protect the rights of the legitimate use of computers and information networks. In the same context, the present study aims to determine different technologies, policies, and actions to provide protection for the information systems for the organizations in Saudi Arabia, the Gulf countries, Middle Eastern countries.

2. Literature Review

The information system usage has expanded significantly within the organizations regardless of their industry. The increased adaptation of the information system has imposed great pressure on the organization involving security and information protection measures. Tomanna et al (2018) have shown that the global competition requires the organization to revamp their functional, tactical as well as strategic procedures in an effective and efficient way. Allen et al (2015) show that the organization today requires an effective information security policy which not only involves a plan but also documents the roles and responsibilities to be followed carried out by the firm personnel for achieving the determined security agendas.

Guo et al (2011) added that the amplified and continuous utilization of the internet and wireless network resources jeopardize the information security system. This is evident from the study conducted by the Ponemon Institute in 2014, which evaluated the economic impact of the cyber-attacks on the economy of United Kingdom, United States, Australia, Japan, Germany, Russia, and France. The results revealed that the overall cost of the breached data was about $12.7 million whereas the lowest cost was found to be $3.3 million (2014).

Although organizations today implement a baseline program for information system security, the number of cyber crimes and data breaches continue to expand. Evidence from the literature provides that about 60% of the organizations are using technological derived security measures for the information system, such as anti-virus software, virtual private networks, software for anti-spyware, firewalls, data encryption in transit, and detection of the intrusion (Ahmad, Maynard & Park, 2014; Richardson 2011). The reports also suggest that these organizations have also experienced attacks on an increasingly frequent basis. Moreover, these studies also highlight that the security risk is significantly expanding as a result of internal as well as external threats. This is making the security management of the organization troublesome.

Considering internal security system threats, it has been recommended by Siponen & Vance (2010) that the firm must improve its efforts for training its workforce with respect to the compliance of the established security policies. It also emphasized on the development of the understanding for the policy breaches among the employees. Furthermore, Hu et al (2011) identified that for ensuring the system security, the punishment alone is not effective. It promotes the development of the high moral stance among the employees as well as increased self-control, which sets the base for the establishment of the security culture. This point is also endorsed by the study of Lim et al (2012), which further emphasizes security culture formation. Kam et al (2013) also identified that the governing, as well as normative external pressure, impact the compliance with the established policies for information security. Son (2011) further added that there is a positive association between the people motivation and the security performance within the organization, which improves the overall security of the organizations.

With respect to the information system security policy, Whitman & Mattord (2014) suggest that these policies can be integrated into the operational procedures of the firm, which are required for the configuration or maintenance of the system such as in the operations of the network firewall. Latham (2013) states that the amalgamation of the key players in the organization with the security policy is important for its implementation and support.

Albuquerque Junior & Santos (2015) point out that every organization needs policies with respect to information system security differences and breaches. For the routine review, monitoring and maintenance of a system must be deployed to look out for the shortcomings (Greene, 2014). Tung (2014) shows that the security measures program and policy must clearly outline the roles and responsibilities of the members to be integrated into the component of accountability.

The organization increased dependence on the information system makes it imperative to improve its protective measures for security system management for safeguarding against the multiple threats. The recognition of the effective use of various technologies, policies, and actions are essential for not only securing the data but also sustaining its effective management.

3. Material and Methods

The study has employed a case study approach to understand the information security system in Saudi Arabia. It was based on the respondent's observations of information security in relation to their culture and experience. The respondents were told to observe the information security weaknesses, the impact of employees' experiences, and organizational culture on the security of the information systems. Analytical research has been conducted using the existing information security system to identify the issues and their causes and effects in a critical evaluation.

Quantitative approach has been used to analyze the collected data through a survey questionnaire. The sample for this study includes male and female staff from a well-known organization in Saudi Arabia. A total of 109 participants were recruited in this survey. The questionnaire used in this study consists of two parts; the first part of the questionnaire gave an idea about the security of the system; while, the second part of questionnaire measured the level of user's information security awareness before and after the implementation of the developed cultural security awareness framework. This questionnaire consisted of 20 questions, which were mostly yes/no and multiple-choice questions, and some more IT security related open-ended questions.

3.1 Data Analysis

The data obtained through the questionnaire has been analyzed using the Statistical Package of Social Sciences (SPSS) version 20.0. The results help in checking the vulnerability of organization's information systems caused by flaws in software and hardware design, weak management processes, lack of awareness or education/training programs, and mishandled upgrading or updating of the current practices.

4. Results

A total of 95 male and 14 female participants, respectively participated in the study (as shown in Table 1). Majority of the study participants belong to the 26-34 years age group. The study also considered the qualification level of the workers, which shows that the majority of the participant were graduates i.e. 50 followed by Masters (26) and Ph.D. (14). The training of the participants was also evaluated in the study as it improves the individual knowledge for effective management of the IT systems (Table 1).

Table 1. Participants Demographic

Variable		N	%
Sex			
	Female	14	12.8%
	Male	95	87.1%
Age		N	%
	Under 20	3	2.7%
	21-25	28	25.6%
	26-34	35	32.1%
	35-40	23	21.1%
	41-45	7	6.4%
	46-50	7	6.4%
	51+	6	5.5%
Qualification		N	%
	High School	19	17.4%
	Bachelors	50	45.8%
	Masters	26	23.8%
	Ph.D.	14	12.8%
Training Courses		N	%
	No	54	49.5%
	Yes (1 course)	25	22.9%
	Yes (1-3 course)	16	14.6%
	Yes (3 or more courses)	14	12.8%
Total		109	100%

The participants were asked about the policies of the organization with respect to the security system protection. Table 2 exhibits the response of the participants which show that majority of the participants do not find any information on the website of the participants whereas participants lack the information or knowledge to access the policies established by the organization. Only 17% of the individuals were able to access the policies and have complete awareness. Majority of the participants agreed that the organization has the policy but 17% were not aware of any policies. When the participants were asked about the security of confidential data on personal device, majority stated that it was not allowed whereas 39% were oblivious to company policy regarding it, and 28% responded that they could store it on a personal device. Overall results show that there is no effective policy of the company for controlling breaches of information security.

Table 2. Organization Security Policy

Questions	Responses	Percentage
Does organization detail the policy out on the website for website security?	No	47%
	Yes	17%
	Yes, but don't know how to access the policies	36%
Does the organization have a policy which provides information on the use of email, such as the purpose of using email and procedure for its usage?	No	33%
	Yes	33%
	Yes, but don't know the policy	15%
	Don't know	19%
Can organization confidential data be stored on employee personal devices such as mobile phone?	No	39%
	Yes	28%
	Don't know	33%

Majority of the participants (39 %) responded that there was no information security team; whereas, 30% responded that there is a security team. Majority of the participants (75%) fails to identify whether their computer is hacked or not; whereas, 25% of the employees identified that their computer is hacked. This provides that the awareness level and the knowledge of the security concerns and issues are lacking among employees (Table 3).

Table 3. Participants knowledge and security awareness

Questions	Responses	Percentage
Does the organization have an information security team?	No	39%
	Yes	30%
	Don't know	31%
Do you know who to contact in case your computer gets infected or hacked?	No	70%
	Yes	30%

Do you know how to identify that the computer is hacked?	No	75%
	Yes	25%
Are you careful while opening an attached email?	Don't open the attachment.	6%
	Open it if it's from a known person.	34%
	Open it irrespective of who the recipient.	60%

A total of 45% participants found virus while 10% of the participants found the virus through their work system. A total of 62% of participants responded that their passwords were shared with other colleagues while 38% said that their passwords were protected by them.

Table 4. Participants experience

Questions	Responses	Percentage
Have you found a virus at your work computer?	Yes	45%
	Never	30%
	Sometimes	15%
	Yes, but don't know how it got infected	10%
Have you shared your work password with your college for someone else?	No	39%
	Yes	61%
Have anyone at work asked you of your work password?	No	38%
	Yes	62%

Table 5. User Practice for System security

Questions	Responses	Percentage
Does your work security system gets automatically updated?	Yes	38%
	No	21%
	Don't know	41%
Have you installed software at your own work computer?	No	70%
	Yes	30%

Are your work and personal account password same?	No	60%
	Yes	40%
Do you take your work information home?	No	47%
	Yes	17%
	Sometime	17%
	Frequently	19%
Do you log into work account using public computers?	No	32%
	Yes	19%
	Sometimes	49%

Table 5 provides responses of the participants with respect to their security practice. Majority of the participants have not installed security practice i.e. 70%, while 30% know how to install the software. When questioned about their password such as whether the participants had their personal and work password same, 60% responded negatively while 40% responded positively. The practice of taking office work home was reported by the majority of participants where 17% frequently take their work home. The public computers are usually infected with the virus; therefore, 32% of participants log into their work account using public computers. Though all these practices may not jeopardize the security system, these pose a great risk to the organization information security system.

5. Discussion

Based on the responses of the participants, it was found that majority of the participants lack the training on the courses essential for proper integration of the security practices in their work. The lack of training hinders their adaptation of information security which tends to improve by undergoing relevant training courses. The results reveal that due to the lack of training among the employees, the system mismanagement prospect increase posing a great security risk. Humaidi & Balakrishnan (2012) supplement this study findings by stating that the system security issues curtail down with the integration of effective training programs. This has been supported by Urhuogo, Addo & Williams (2014) who found that integration of proper scheduled training program leads to the improved security measures for the IS system. Integration of proper scheduled training program leads to the improved security measures for the IS system (Urhuogo, Addo & Williams, 2014).

The formation of the security policy is not enough for the effective controlling of the information security issues. The responses of the individuals show that the websites of the company fail to provide individuals with information for securing their system. This impacts the company's effective adaptation of the practice and actions as per the policy, impacting their security of the information system. Alzahrani & Alomar (2016) found parallel results to the present study providing that website serves as a great source for raising the employee awareness and overcoming the security threats.

The security measure practices are also impacted by the lack of awareness of the employees about the company. This is evident from the responses which show that the majority of the participants are unaware of the security policies formulated by the firm. The lack of awareness causes individuals to breach it. The deficiency of IS security policy has also been examined by Alshaikh et al (2016), which highlighted that for meeting the determined security measures, the awareness of the policy is integral. The solution suggested for overcoming it includes providing new modes of communication either through email, end users or in the form of feedback. The improved communication ensures that the organization meets the necessary standard set as a part of its security policy. The storage of company data on personal devices is also recognized as another factor hindering the effective implementation of

the security policy.

The lack of awareness about the information security policy and security measures among the employees is also evident from the employees' lack of capacity to detect the skill or lack of knowledge on who to contact in case it is identified. Along with it, the study also highlighted that inability of the employee to install or run the antivirus also contribute towards the issues of the security system. The high expectation and trust among the colleagues can also affect the security information system of the company. Such as the lack of awareness among the employees of the security policy can lead to the password sharing practices which increases the security concerns.

The use of public platforms or computers for work account also puts the information system into jeopardy. Since multiple individuals use these systems, the virus probability is high. The use of public platforms for accessing the information system of the firm must culminate. This has further been stressed by Ismail & Zainab (2013), who found that increased usage of the public platforms impacts the security of the information system.

Along with it, using the same password for both personal and professional accounts increase the hacking prospects. Such as, the hacker through the personal account password is able to access the office account and steal the pertinent organization information. The study suggests making employees aware of the tactics which may be adopted by hackers. Alzahrani & Alomar (2016) further emphasizes that more details must be shared with the employees related to password security and practices which help in mitigating the hackers attack. Ruoti, Andersen & Seamons (2016) elucidated that information related to password strength must also be shared with the organization employees to eradicate their practice of using weak passwords. The present study further suggests introducing programs for raising employee password awareness. The study has also provided solutions such as initiating programs for increasing employee awareness as it assists employees to realize the significance of the information and its security system. The organization must also introduce practices as allows it to elucidate the danger which and tackle it as a result of information misuse.

It is emphasized in the current study, to regularly audit the information system, improve the employee knowledge for the identification of threats, detect the virus attack, and understate the course of action to be adopted along with the information and risks classification. The adaptation of collaborative work practice will assist the organization in overcoming the prevailing information system security issues and threats. At this juncture, the study concludes that improving the employee knowledge of the information system contributes to the enhancement of the information system. The implementation of the security policies along with proper knowledge and awareness is required for enhancing the information system security. Information system security requires the development of the framework which integrates into necessary guidelines for the implementation of the information security policies. The security system practices and deficiencies serve as a guideline for the management to construct benchmark security policies and allow the employees for a better understanding of the process.

Few limitations of the study are observed such as the study was confined to one region only. The constraints of a region limit the generalization of the results. Additionally, it also suggests that future study can undergo a qualitative study design and include organizations from various regions. The SME information security can also be explored for determining the impact of different technologies, policies, and actions. Moreover, the gender understanding of the information system can also be explored with regard to the information system security.

Conflict of Interest

The authors declare that they have no conflict of interest.

Ethical Approval

This article does not contain any studies with human participants performed by any of the authors.

References

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing, 25*(2), 357-370.

Albuquerque Junior, A. E. D., & Santos, E. M. D. (2015). Adoption of information security measures in public research institutes. *JISTEM-Journal of Information Systems and Technology Management, 12*(2), 289-315.

Allen, J. H., Crabb, G., Curtis, P. D., Fitzpatrick, B., Mehravari, N., & Tobar, D. (2015). Structuring the chief information security officer organization (No. CMU/SEI-2015-TN-007). CARNEGIE-MELLON UNIV PITTSBURGH PA PITTSBURGH United States.

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2016). Information Security Policy: A Management Practice Perspective. arXiv preprint arXiv:1606.00890.

Alzahrani, A., & Alomar, K. (2016). Information Security Issues and Threats in Saudi Arabia: A Research Survey. *International Journal of Computer Science Issues (IJCSI), 13*(6), 129.

Babaei, M., & Beikzad, J. (2013). Management information system, challenges, and solutions. *European Online Journal of Natural and Social Sciences: Proceedings, 2*(3s), 374.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548. https://doi.org/10.2307/25750690

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management, 29*(6), 449-457. https://doi.org/10.1016/j.ijinfomgt.2009.05.003

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & security, 31*(8), 983-988. https://doi.org/10.1016/j.cose.2012.08.004

Greene, S. S. (2014). Security Program and Policies: Principles and Practices. Indiana: Pearson IT Certification.

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.

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), 54-60.

Humaidi, N., & Balakrishnan, V. (2012). The influence of security awareness and security technology on users' behavior towards the implementation of health information system: A conceptual framework. In 2nd International Conference on Management and Artificial Intelligence IPEDR (Vol. 35, pp. 1-6).

Ismail, R., & Zainab, A. N. (2013). Information systems security in special and public libraries: An assessment of status. arXiv preprint arXiv:1301.5386.

Kam, H.-J., Katerattanakul, P., Gogolin, G., & Hong, S. (2013). Information Security Police compliance in higher education: a neo-institutional perspective. Proceedings of Pacific Asia Conference on Information Systems, Jeju Island, South Korea, 17.

Kim, D. W., Yan, P., & Zhang, J. (2015). Detecting fake anti-virus software distribution web pages. *Computers & Security, 49*, 95-106. https://doi.org//10.1016/j.cose.2014.11.008

Latham, R. (2013). Information Management Advice 35: Implementing Information Security.

Lim, J. S., Chang, S., Ahmad, A., & Maynard, S. (2012). Towards an organizational culture framework for information security practices. In Strategic and practical approaches to information security governance: Technologies and applied solutions (pp. 296-315). IGI Global.

Ponemon Institute. (2014). *2014 Cost of Data Breach. IBM.* Retrieved November 12, 2018, from http://www935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

Richardson, R. (2011). 2010/2011 CSI Computer Security Crime & Security Survey. Computer Security Institute.

Ruoti, S., Andersen, J., & Seamons, K. E. (2016, June). Strengthening Password-based Authentication. In Way@ Soups.

Safa, N. S., & Ismail, M. A. (2013). A customer loyalty formation model in electronic commerce. *Economic Modelling, 35*, 559-564. https://doi.org/10.1016/j.econmod.2013.08.011

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly,* 487-502.

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48*(7), 296-302.

Tomanna, T., Gerbi, D. Y., Hossin, M. A., & Zhang, S. (2018). Impact of Information System on Transformation of Human Resource Performance: An Exploratory Study in Oromia Radio and Television Organization. *Journal of Human Resource and Sustainability Studies, 6*(01), 37.

Tung, L. (2014). IT security governance: Boards must act. Retrieved November 12, 2018, from http://www.zdnet.com/article/it-security-governance-boards-must-act

Urhuogo, I., Addo, A., & Williams, D. (2014). The influence of information systems security on job performance: A proposed research topic. *Journal of Business Studies Quarterly, 6*(1), 191.

Whitman, M., & Mattord, H. (2014). *Management of information security.* Boston: Course Technology Cengage Learning.