Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 124 (2017) 691–697

Procedia Computer Science

www.elsevier.com/locate/procedia

4th Information Systems International Conference 2017, ISICO 2017, 6-8 November 2017, Bali, Indonesia

Developing an Information Security Policy: A Case Study Approach

Fayez Hussain Alqahtani*

King Saud University, P. O. BOX 2454, Riyadh 11451, Kingdom of Saudi Arabia

Abstract

Organisational information and data must be protected from active and passive attacks and secured from illegal access, unwanted interruption, unauthorised alteration or annihilation. Many organisations fall victim to such attacks due to weak information security policies (ISPs). Also, disrupting these IS policies by IT users makes organisations under information security threats. This study explored the implementation of ISPs within a large organisation to evaluate policy adequacy and to determine user awareness and compliance with such policies. Employing a case study approach, this research found that the information security focus areas included in this organisation ISPs are password management; use of email, the Internet and social networking sites; mobile computing; and information handling. However, the maturity levels of these elements varied among focus areas due to a lack of ISP awareness and compliance among users.

Peer-review under responsibility of the scientific committee of the 4th Information Systems International Conference 2017.

Keywords: Information Security; Information Security Policy; IS Awareness; ISP Maturity; Case Study.

1. Introduction

Information security (IS) remains one of the critical concerns for modern organisations. Organisational information and data must be protected from both active and passive attacks [1]. Every organisation should secure data from illegal access, unwanted interruption, unauthorised alteration or data annihilation [2]. IS emphasises confidentiality, integrity and availability of data, which play vital roles in securing organisational data and should be properly implemented [3]. However, in many organisations, people unconsciously disrupt these IS policies (ISPs) due to lack of awareness about related terms and conditions, which heightens the risk of IS attacks [4–6]. This study

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
E-mail address: fhalqahtani@ksu.edu.sa

1877-0509
Peer-review under responsibility of the scientific committee of the 4th Information Systems International Conference 2017
10.1016/j.procs.2017.12.206

explores the implementation of ISPs at an educational institution within an Arab gulf country, as well as user awareness and compliance with such policies.

The remaining of this paper is structured as follows. The coming section provides background information on IS, threats to IS and Information Security Policy (ISP) by reviewing a selection of existing works on topics related to requirements for ISPs. Then, a framework is identified to evaluate the design of IS policy. The third section describes the research methodology, including data collection and data analysis methods. The next section discusses the study results and compares these to results found in the literature. Finally, summaries of the study's contributions and implications for stakeholders are presented.

2. Literature Review

2.1. Information Security

IS has received much attention because security is a key concern when introducing information and communication technologies within organisations [7]. Platforms for IS protect organisational data from various attacks and are able to identify susceptibilities of outliers and threats to data [8]. Data must be protected from both active and passive attacks; thus, IS emphasises confidentiality, integrity and availability, according to Tchernykh [9]. Confidentiality refers to privacy, integrity to upholding the constancy, correctness and dependability of data and availability to 24/7 data access. Properly implemented IS not only plays a vital role in securing organisational data but also provides methods for data storage. With growing demand for IS, many authors have stressed the importance of eliminating weaknesses, which are apparent in many organisations [3–4]. Such weaknesses appear when people unconsciously disrupt ISPs due to lack of awareness about related terms and conditions, resulting in socially, economically and physiologically questionable actions, as noted in [5] and [6].

2.2. Threats to Information Security

Unforeseen or undesirable events with harmful consequences for organisations can be referred to as threats, and IS threats can be both internal and external [10]. Internal threats are caused by people working within an organisation, primarily due to unprotected private access to organisational information about operations and processes [11]. External threats come from entities outside an organisation. Implementation of ISPs is negatively affected by human error, which is the most common issue when applying ISPs [12–14]. For example, unintentional data entry, editing or modification may lead to social, economic or physiological losses, which are challenging issues to manage. Human error can also include rigidness in user behaviour related to accepting ISPs. This rigidness can lead to alterations in human performance, causing deviations from preferred success paths and resulting in unplanned results [15]. An organisation must address all possible human errors while writing ISPs because such errors can be critical for any organisation if not handled competently [13]. Major causes of the occurrence of human errors include lack of knowledge or skills related to IS [14]; thus, managing human error in any organisation is vital, and errors must be taken as a serious threat. As such, it is essential to introduce ISPs to all stakeholders, including end-users, of an organisation to ensure compliant behaviour.

2.3. Information Security Policy

ISP supports appropriate behaviour among employees by providing clear instruction of responsibilities to follow terms and conditions of such policies [16]. Employees who properly follow ISPs are assets to organisational security [17]. ISP bridges the gap between the expectations of an organisation and how people contribute to the proper implementation of ISP, which should be very clear to understand and implement. Additionally, ISPs are often created for employees, who should always be considered during the policy development process [17–18]. Various organisations use jargon in such policies that makes it difficult for new users to understand and implement ISPs; therefore, policies should be clear enough to help employees follow organisational terms, even during exceptional circumstances [19]. A weak ISP design may result in lack of protection for subtle data or it may cause employees to do detrimental actions to their organisations. After validating the strength, scope and practical application of ISPs,

policies should be regularly examined and evaluated according to defined standards for periodic improvements. Therefore, the requirement paradigm for ISPs should be a focus during policy design and iterative check-ups.

2.4. Requirements of Information Security Policy

Clear and practical ISPs can help organisations improve IS programmes. After designing and developing an ISP, an organisation should frequently observe and address any variances that may arise in IS assets [3]. These intermittent observations can help organisations determine if the continuance alteration in organisational structure or procedures influences the effectiveness of its ISPs [20]. Keeping in mind organisational security objectives, ISP compliance behaviour should not hinder an organisation in terms of safeguarding data and information security [16]. Parsons et al. [14] reviewed many ISPs and interviewed professionals to discuss IS with the management of organisations to determine the key requirements and focus areas that should be considered while developing an ISP. After this process, seven focal areas were identified for designing and testing ISPs (Table 1).

Table 1. Information Security Focus Areas.

ISP focus areas	Sub-areas
Password management	Locking workstation Password sharing Choosing a good password
Email use	Forwarding emails Opening attachments IT department's level of responsibility
Internet use	Installing unauthorised software Accessing dubious websites Inappropriate use of the Internet
Social networking site (SNS) use	Amount of work time spent on SNS Consequences of SNS
Mobile computing	Sending sensitive information via mobile networks Checking work email via free networks
Information handling	Disposing of sensitive documents Inserting DVDs and USB devices Leaving sensitive material unsecured

This research is advised by Parsons's work [14] that reviewed several information security policies to develop specific focus areas, which are the areas of ISP that are to a great extent relevant to IT users and employers, as well as to noncompliance behaviours. These focus areas are used as an evaluation tool for ISP in some institutions; thus, these areas have been used to develop interview protocols to collect data from the heads of information technology (IT) at the institution studied here.

3. Research Methodology

A case study is one way of conducting social science research that allows real-life investigations [21]. Such studies can be exploratory, as in the current research, in which a case study was used to discover the state of qua of ISP at an educational institution and to explore user awareness and compliance with such policies. There are two phases to this research. First, an extensive review of ISP documents from the selected institution was conducted using the focus areas from [14] as an appraisal model. The aim of this phase was to evaluate the maturity level of developing and formulating ISP. Four levels of maturity were used: 0 = nonexistence, 1 = existence, 2 = + acceptable use and 3 = ++ reporting procedure. Second, qualitative research was conducted using semi-structured interviews with four IT units' managers. Experienced IT managers from different divisions were selected to understand the practise of IS and to verify compliance with ISP. Interviewing relevant managers provided a clear picture of the business, reproducible results and consistency, while reviewing documentary evidence verified compliance level. The Appendix presents the interview protocol used in this study.

4. Findings

4.1. Review of Information Security Policy (ISP)

This research found that the IS focus areas included in the study organisation's ISP were password management, Internet use, email use, mobile computing, SNS use and information handling. Yet, the maturity level of developing and formulating policy elements varied among these focus areas, as the following table shows. For example, password management had a higher level of maturity compared to mobile computing.

Table 2. Maturity of ISP

ISPs focus areas	Sub-area	Evaluation	Maturity
Password management	Locking workstation	1	Below average
	Password sharing	3	Good
	Choosing a good password	3	Good
Email use	Forwarding emails	0	Poor
	Opening attachments	2	Average
Internet use	IT department level of responsibility	1	Below average
	Installing unauthorised software	2	Average
	Accessing dubious websites	0	Poor
	Inappropriate use of the Internet	3	Good
SNS use	Amount work time spent on SNS	1	Below average
	Consequences of SNS	0	Poor
Mobile computing	Sending sensitive information via mobile networks	2	Average
	Checking work email via free networks	0	Poor
Information handling	Disposing of sensitive documents	1	Below average
	Inserting DVDs and USB devices	0	Poor
	Leaving sensitive material unsecured	1	Below average

Note: 0 = nonexistence, 1 = existence, 2 = + acceptable use, 3 = ++ reporting procedure

4.1.1. Password management

ISP addresses how passwords are changed and explains the different steps users can follow to change their passwords as the best practices related to password management, such as changing passwords regularly, selecting a strong password and preventing passwords from been shared with other users. This review revealed that the current ISP at the institution does not specify a subarea for locking workstations, while other password management subareas were scattered throughout various ISP documentation, such as the acceptable use policy document.

4.1.2. Email use

The general responsibilities of IT departments are defined in a number of ISP documents; however, there is a need to specify IT responsibilities relating to email use to help users resolve issues such as fishing emails. Although it is critical, the issue of forwarding emails does not exist in any ISP document at the institution. The automatic forwarding of official emails from work mail servers to external email accounts introduces security risks, such as loss of control over sensitive work-related information. Finally, the current ISP provides email issues within acceptable use documentation, along with other security issues.

4.1.3. Internet use

In a number of ISP documents, users are warned to avoid inappropriate use of the Internet, which includes the use of institutional infrastructure and portals and discussion boards to discuss sensitive non-work related matters. An entire ISP document extensively discusses the appropriate use of work portals and websites. Additionally, the institution states that it has the right to monitor users' generated content to ensure internet use is in accordance with the ISP. The institution does not mention the use of other public websites or virtual communities to discuss work-related matters. Finally, in some parts of the ISP, users are prohibited from downloading any software apart from licensed products made available in the central IT department portal.

4.1.4. Social networking sites

The use of SNS receives minimal attention in the institution's ISP, which appoints a specific department to work on the institution's social media accounts (e.g., Facebook and Twitter) for public relations purposes. Discussion regarding appropriate use of these SNS, the consequences of use and potential security threats should be included in

the ISP. The institution has its own social media application, and the ISP includes a specific policy document to outline the purpose of this application and the practical steps for using it.

4.1.5. Mobile computing

In an ISP document named 'Access Police', the need to manage mobile work activities through secured institutional devices and virtual networks is discussed. Extensive discussion regarding international mobile networks and public Wi-Fi networks should also be included in this policy, including what type of activities are allowed on such networks and whether logging onto work email through these networks is safe.

4.1.6. Information handling

Attention to information handling is minimal in the current ISP documents. A short note regarding the disposal of work documentation and records indicates that this is allowed after a specific amount of time; this note is found in an ISP document titled 'Commitment Policy'. However, the documents titled 'Leaving Sensitive Material Unsecured' and 'Access Police' include the same note. This policy suggests that workers continually clean their offices and dispose of sensitive documents regularly.

4.2. ISP Awareness and Compliance

Participants interviewed in this research were IT managers of entire divisions, who reported to the deputy directors of each division rather than the IT main office. The role of these managers was to maintain the IT infrastructure and ensure the quality of IT services. This study found that the distributed IT managers were not involved in the development process for ISP due to a centralised working culture and the current organisational structure. The IT main office had full ownership of the ISP, as noted in the interviews: *'The main IT office in headquarters developed the IS policy some time before and is responsible for ensuring its implementation'* (n2), and *'I am not sure, but I think there is an IS policy'* (n1). This resulted in a lack of awareness of the current ISP among IT unit managers. One manager stated:

> *'I don't know much about the information security policy, but I am sure we have an IS policy developed by our IT main office, but I could not comment on it or its usability as I have not accessed it yet.'* (n3)

Occasionally the main IT office sent warnings via email that included sections of its ISP to inform users might of the policy or *'when users have an IT issue, and they call the main IT office to resolve this issue'* (n2). This is insufficient, and the institution should run an IS awareness programme, particularly when *'observing the number of security threats caused by users' lack of awareness'* (n4). Examples of these threats include *'accessing prohibited websites'* (n4), *'using old versions of anti-virus software'* (n1), *'downloading unauthorised software or files'* (n2), *'uploading infected files to the intranet'* (n2), *'receiving suspicious emails and opening their attachments'* (n3) and '*taking work computers for maintenance outside the institution'* (n1).

Therefore, most participants agreed that there was a need to include important information for users about appropriate use of email and Internet as well as other related IT systems in the institutions ISP. They also noted that ISP should include a practical guide on how to use IT infrastructure in a secure manner.

5. Discussion and Conclusion

IS focus areas included in this study were password management, Internet use, SNS use, email use, information handling and mobile computing, which were present in the policy of the case institution. However, these subareas had various maturity levels in regards to policy discussion and guidance. For example, password management had a higher level of maturity compared to mobile computing. Under these major subareas, there were sixteen subareas, including choosing good passwords, locking workstations, opening email attachments, forwarding emails, checking work emails via free networks, installing unauthorised software, accessing dubious websites, inappropriate use of the Internet, IT department level of responsibility, amount of work time spent on SNS, consequences of SNS use, sending sensitive information via mobile networks, inserting DVDs and USB devices, disposing of sensitive

documents and leaving sensitive material unsecured. The maturity levels of these subareas varied as follows: three were good, three were average, five were below average and five were poor.

The policy articulation of aspects such as forwarding emails, accessing emails via unsecure wireless networks, accessing dubious websites and using SNS were weak and should be more carefully considered in the ISP because lack of such aspects can lead to harmful security results and expose individuals, teams and units to possible attacks. Another security area that requires careful consideration is information handling, which includes inserting DVDs and USB devices, disposing of sensitive documents and leaving sensitive material unsecured by leaving workstations for example unlocked. Confidential electronic and paper information must be secured and inaccessible to unauthorised individuals. Furthermore, formatting the ISP is critical to ensure policies are properly followed and understood as useful tools by users. The minimum requirements for formatting an ISP is to introduce and define acceptable use, the security focus and sub-focus areas and reporting procedures for security breaches.

Distributed IT managers were disconnected from the ISP and were unfamiliar with it because they had not participated in policy development, which meant that they could not adequately support the policies' strengths or enhance its weaknesses. Their involvement is crucial because they are experts in current IS issues. This might be the main reason for the low maturity level of many of the IS subareas in the institution under study. Additionally, having full ownership of and maintaining the ISP would encourage the distributed IT managers working in the field to consider IS matters irrelevant to their jobs, while observing IT systems usage and correcting unwanted behaviour that might cause IS threats. IT managers need to feel more engaged to be motivated in planning and executing IS awareness programmes in cooperation with the IT main office. This cooperation should result in a clear and organised guide to maintaining IS and using IT infrastructures and services in a secure manner.

This study explored the implementation of ISP within a large organisation to evaluate the current ISP and IS awareness and compliance among employees. There were various maturity levels detected for ISP focus areas at this institution, and many subareas were ranked below average. Formatting the ISP is critical to ensuring that users understand and follow the policy. Compliance with the ISP was low due to the disconnection between distributed IT managers and the main IT office in relation to ISP development and deployment. Future research could survey several groups of end users, such as students, faculty members and administration, to understand and compare their IS practises. Using a design science approach in future research could help develop a more appropriate format for ISP that is useful and easy to use.

Appendix A. Interview Protocol: Information Security Policy

Education:
Job Role:
Years of Experience:

What are your organisation's policies that explain information security requirements?

How have these policies been developed?

How easy to follow are these policies for users?

How are users made aware of the existence and the importance of these policies?

What are the most important issues of information security and acceptable use of network systems and information resources in your organisation?

What are the advantages of the documents written in your organisation that explain the information security policies?

What are the most important aspects that require further development in these information security policy documents?

References

[1] Peltier TR Information security policies and procedures: A practitioner's reference. 2nd ed. Auerbach Publications; 2004.
[2] Warkentin M, Willison R. Behavioral and policy issues in information systems security: The insider threat. European Journal of Information Systems 2009;18**:**101–105.
[3] De Lange J, Von Solms R, Gerber M. Information security management in local government. In: Cunningham P, Cunningham M, editors. 2016 IST-Africa Week Conference, 11-13 May 2016, Durban, South Africa: IIMC International Information Management Corporation; 2016, p. 1–11.
[4] Kadam AW. Information security policy development and implementation. Information Systems Security 2007;16:246–256.
[5] Vroom C, Von Solms R. Towards information security behavioural compliance. Computers & Security 2004;23**:**191–198.
[6] Johnston AC, Warkentin M, Mcbride M, Carter, L. Dispositional and situational factors: Influences on information security policy violations. European Journal of Information Systems 2016;25**:**231–251.
[7] Pang M.-S, Tanriverdi H. Security breaches in the US federal government. 2017 [Online] Available: http://dx.doi.org/10.2139/ssrn.2933577
[8] Layton TP. Information security: Design, implementation, measurement, and compliance. CRC Press; 2016.
[9] Tchernykh A, Schwiegelsohn U, Talbi, E-G, Babenko M. Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. Journal of Computational Science 2016;Vol:page numbers.
[10] Cavusoglu H, Cavusoglu H, Son J-Y, Bbenbasat I. Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. Information & Management 2015;52:385–400.
[11] Jouini M, Rabai LBA, Aissa AB. Classification of security threats in information systems. Procedia Computer Science 2014;32:489–496.
[12] Gerić S, Hutinski Ž. 2007. Information system security threats. Journal of Information and Organizational Sciences 2007;31:51–61.
[13] Liginlal D. HIPAA and human error: The role of enhanced situation awareness in protecting health information. In: Gkoulalas-Divanis A, Loukides G, editors. Medical data privacy handbook, Springer International Publishing; 2015.
[14] Parsons K, Mccormac A, Butavicius M, Pattinson M, Jerram C. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security 2014;42:165–176.
[15] Wood CC, Banks WW. Human error: An overlooked but significant information security problem. Computers & Security 1993;12:51–60.
[16] Siponen M., Mahmood M, Pahnila S. Employees' adherence to information security policies: An exploratory field study. Information & Management 2014;51:217–224.
[17] Flowerday SV, Tuyikeze T. Information security policy development and implementation: The what, how and who. Computers & Security 2016;61:169–183.
[18] Yazdanmehr A, Wang J. Employees' information security policy compliance: A norm activation perspective. Decision Support Systems 2016;92:36–46.
[19] Doherty NF, Anastasakis L, Fulford H. The information security policy unpacked: A critical study of the content of university policies. International Journal of Information Management 2009;29:449–457.
[20] Pattinson M, Butavicius M, Parsons K, Mccormac A, Calic D. Managing information security awareness at an Australian bank: A comparative study. Information and Computer Security 2017;25:181–189.
[21] Yin RK. Case study research: Design and methods. CA, USA: Sage Publications; 2013.