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.

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

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,