International Journal of Information Management 43 (2018) 165–172

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

Understanding key skills for information security managers

Husam Haqaf, Murat Koyuncu

Information System Engineering, Atilim University, Ankara, Turkey

ARTICLE INFO

Keywords:
Information security management
Security skills
Information security manager
Security certifications

ABSTRACT

Information security management is a necessity for all institutions and enterprises that regard company information as valuable assets. Developing, auditing and managing information security depends upon professional expertise in order to achieve the desired information security governance. This research seeks the key skills required for the position of information security management as well as the methods to develop these skills through professional training programs. The study adopts the Delphi method which requires building a list of items through a literature survey and involves experts with certain expertise to modify the list until a consensus on less than 20% of the items is reached. Through completing three rounds of the Delphi technique - data collection, relevance voting and ranking - sixteen skills are shortlisted as the key skills. In the final list, the majority belong to core information security skills, and the top two skills belong to project/process management skills and risk management skills, indicating the importance of these skills for the information security manager role. In addition, a series of related professional training programs and certifications are surveyed, the outcome of which highlights a number of most comprehensive and appropriate programs to develop these determined skills.

1. Introduction

An Information Security Management System (ISMS) is a set of standards, by which companies can protect their vital information assets in certain industries such as healthcare (Gardiyawasam Pussewalage & Oleshchuk, 2016) and finance (Roumania, Nwankpab, & Roumani, 2016). It mainly focuses on closing the gap in the security systems and processes through risk management (Bojanc & Jerman-Blazic, 2008; Silva, De Gusmão, Poleto, Silva, & Costa, 2014). Moreover, the process was standardized via the ISO/IEC 27001:2005 (later, revised by ISO/IEC 27001:2013) based on the British Standards BS 7799 and developed by the UK's Department of Trade and Industry (Humphreys, 2016). The implementation of ISO/IEC 27001 is based on examining various core concepts that are treated either solely or combined, and includes the context of organizations, issues, risks, opportunities, interested parties, leadership, threats, communication, documented information, performance evaluation, risk owners, risk treatment plans, controls, and continual improvement. In this respect, risk management plays a major role in implementing this standard as it should always be planned, controlled and assessed.

Information security provides a way to protect the valuable assets of any organization, especially the ones that hold sensitive information. It is based on three main principles, which are (ISO/IEC, 2013):

1 Confidentiality: preventing unauthorized access to sensitive data;
2 Integrity: truthfulness of the data, which cannot be modified without authorization; and
3 Availability: accessibility of the data whenever it is requested by authorized personnel.

Information security owes its importance to several issues, especially from the legal point of view. As governmental services increasingly become online day by day, a large amount of vital information about individuals and governments could be at risk in different parts of the world without the presence of security systems (Ozkan & Karabacak, 2010; Saarenpaa, 2008). Studies show that, in an organization, there are many business-related highlights to be considered in ISMS which include, and are not limited to:

1 Preserving information within the organization in order to maintain competitiveness in the market;
2 Sustaining growth by making the needed information available at all times to the company's decision-makers; and
3 Enhancing communication systems within the organization to support efforts towards stability (Wawak, 2010).

The information security manager (ISM) is a managerial role related to information security and is different from the information security expert with regard to function. The ISM is mainly responsible for:

E-mail address: mkoyuncu@atilim.edu.tr (M. Koyuncu).

https://doi.org/10.1016/j.ijinfomgt.2018.07.013
Received 7 March 2018; Received in revised form 30 July 2018; Accepted 31 July 2018
0268-4012/ © 2018 Elsevier Ltd. All rights reserved.

1 Ensuring that security processes, systems, policies, standards and guidelines are established, communicated and improved across the entire organization to protect information assets;
2 Making security-related decisions;
3 Collaborating with internal and external stakeholders for all operations; and
4 Supervising the security experts' teams.

As stated before, information is an important asset for organizations. On the other hand, organizations are becoming more and more connected. As a consequence, information is exposed to a growing number and a wider variety of threats and vulnerabilities. Therefore, effective information security management becomes a necessity for today's organizations (Furnell, Fischer, & Finch, 2017; Soomro, Shah, & Ahmed, 2016) and, for this purpose, the ISM has the most critical role in an organization. With this in the background, the current required skills for ISMs need to be investigated to examine their compatibility with the requirements of the general framework as well as the predicted market demands. Although there are different resources providing information about these skills, the following problems still exist:

1 There are different skills proposed by different resources. Therefore, it is difficult to decide which one is more appropriate.
2 When the proposed skills from different resources are combined, a very extended list appears, making it difficult to prioritize the most important items.
3 Technology and the related requirements are changing and, dependably, security threats and vulnerabilities are also changing in parallel. Therefore, there is a necessity to have an ever-present and updated list of skills available.

The aim of this study is to review the competitive frameworks in the ISMSs and to understand the key skills to be acquired by ISMs in order to maintain competitive advantage. Therefore, the main research questions of this study are:

- What are the most important key skills to be possessed by ISMs as required by different ISMS frameworks and in accordance to market demands?
- How can these skills be developed through professional certifications offered in the domain?

In this scope, the present research determines the key skills for ISMs, and also the methods to acquire these key skills through professional certifications. The study uses the Delphi method (Dalkey, 1963), which allows filtering the skills and concluding the most important items based on experts' consensus. The method is implemented in three rounds: data collection, relevance voting and ranking. In the first round of this research, ISMSs and major related frameworks are studied in order to extract the skills and competencies that security managers should either possess or develop. The theoretical review performed within this step of the study is confirmed with a field survey of sector professionals in order to conclude the main skills needed for the ISM role. In total, 82 skills are collected as the output of the data collection round. Following the second and third rounds, the top 20% of the filtered skills achieving a minimum score of 3.25 on a 7-point scale are ranked and finalized as the key skills for the role of ISM. In addition, IT security-related certifications are investigated to find out how an ISM can acquire the determined key skills.

2. Literature review

2.1. ISMS objectives and skills

An ISM oversees the protection of hardware and software assets, networks and data against any threats including breaches and criminal acts (Linton, 2013). A survey through the literature reveals that the required ISM characteristics to be possessed are beyond the ones required for the three-main objectives of security systems, i.e. confidentiality, integrity and availability. The list details these tasks to include, and not be limited to providing accountability, security policy, assets control, continuity and solid operations (Da Veiga, 2016; Fenz, Heurix, Neubauer, & Pechstein, 2014; Ma, Johnston, & Pearson, 2008).

Furthermore, as human errors and failures appear even in top risk scenarios in information security management (Ng, Ahmad, & Maynard, 2013), some studies have attempted to sum up the required skills for IT professionals and, specifically, for ISMs. In a survey conducted in six organizations in the United States to determine the basic key skills expected from IT professionals, 14 were identified with regard to the information security individuals' core knowledge (McMurtrey, Downey, Zeltmann, & Friedman, 2008). According to the results, a strong knowledge of languages entails the top requirements within the surveyed organizations and professionals. Moreover, among the professionals within the information security field, those at different organizational levels are expected to have a knowledge of ISMS practices. They are not only supposed to understand the ISO and framework guidelines, but also manage, design, implement and evaluate different components of technical and managerial systems at different levels (Gleghorn & Gordon, 2012).

The different tasks to be undertaken by IT security specialists should be in accordance to seniority and position, and their roles can be classified as executive, operational or productive. The tasks of the executive role mainly require management, design and evaluation. However, the operational and productive roles mainly require implementation of the IT security design, with less management, design and evaluation. Therefore, the ISM's role falls under the executive position and is responsible for putting into action the plans and policies of the top management of a company (Gleghorn & Gordon, 2012).

There are many certifications offered within information and IT security frameworks that specify the development, processes, policies and assessment criteria of a security system. There are also many skills that can be taken from these frameworks, henceforth making it is a challenge to be inclusive in this respect. Nevertheless, there is a consensus that the source of this difficulty is that an ISM has an unavoidable conflict due to being a technical specialist with a managerial role, where he or she needs to discuss issues, understand the users, and negotiate possibilities. Therefore, he or she always has to find the balance where an educational approach can be used without compromising corporate interests (Ashenden, 2008).

There are several frameworks and certification programs that set the standards for due processing and certifying all IT security professionals. According to Gleghorn and Gordon (2012), security managers that acquire specific certifications develop the following advantages:

1 More probability for promotion within the information security organization structure;
2 Better technical skills than those with lower or no certification in the information security field; and
3 Becoming a valuable asset for the organization as they help to save time and money for the entire establishment.

When studying the key skills required for ISMs, it is necessary to understand the type of qualifications needed to operate, manage and maintain these frameworks. Therefore, it is important to take into account the skills required by ISMs according to different frameworks.

The Information Systems Audit and Control Association (ISACA) has noted, in its report on ISM position requirements, that the role of security professionals tends to evolve into a business-oriented format as they advance in their careers. A survey result obtained from security managers, who indicated the percentage of their current job activities in comparison with their previous years, shows that many business-oriented activities have climbed up in the responsibility matrix as part

Download English Version:

https://daneshyari.com/en/article/7428941

Download Persian Version:

https://daneshyari.com/article/7428941

Daneshyari.com