Chapter 36
Enterprise Information Security Policies, Standards, and Procedures:
A Survey of Available Standards and Guidelines

Syed Irfan Nabi
Institute of Business Administration, Pakistan & King Saud University, Saudi Arabia

Ghmlas Saleh Al-Ghmlas
King Saud University, Saudi Arabia

Khaled Alghathbar
King Saud University, Saudi Arabia

ABSTRACT

This chapter explores enterprise information security policies, standards, and procedures. It examines the existing resources, analyses the available options, and offers recommendations to the CIOs and other people that have to make decisions about policies, standards, and procedures to ensure information security in their enterprise. Additionally, the need, requirements, and audience for different types of security documents are scrutinized. Their mutual relationship is examined, and the association among them is illustrated with a diagram supplemented by an example to bring about better comprehension of these documents. It is important to know the sources and organizations that make standards and guidelines. Therefore, the major ones are discussed. This research involved finding all of the relevant documents and analyzing the reasons for the ever-increasing number of newer ones and the revisions of the existing ones. Various well-known and established international, as well as national, information security standards and guidelines are listed to provide a pertinent collection from which to choose. The distinguishing factors and common attributes are researched to make it easier to classify these documents. Finally, the crux of the chapter involves recommending appropriate information security standards and guidelines based on the sector to which an organization belongs. An analysis of the role played by these standards and guidelines in the effectiveness

DOI: 10.4018/978-1-4666-4707-7.ch036

of information security is also discussed, along with some caveats. It is important for practitioners and researchers to know what is available, who the key players are, and the potential issues with information security standards and guidelines; they are all concisely presented in this chapter.

INTRODUCTION

Various facets of human life have undergone tremendous change because of technological advancements, especially in information and communication technologies (ICT). Information systems and communications networks, which are integral parts of these ever increasing information collection, processing, storage, and transmission activities, are becoming more and more attractive targets for malicious attacks by individuals, groups, and even organizations backed by nation states as another arena of warfare–cyberspace and a new type of war–information warfare. A recent example was the cyber attack on Iranian nuclear installations using a worm ("Stuxnet worm hits Iran nuclear plant staff computers," 2010; "Kaspersky Lab provides its insights on Stuxnet worm," 2010). There have been numerous incidents of cyber attacks on information systems and networks and the reported losses from these are increasing (PricewaterhouseCoopers, 2010).

Organizations need to effectively and proactively deal with these risks of potential attacks on their information systems and assets by providing appropriate measures in the form of systems, resources, policies, and programs to counter such risks. Responding to this need, numerous information security-related companies have developed and provided various off-the-shelf solutions. Although this seems to have simplified the tasks faced by organizations by allowing them to pick and choose whatever solutions best suit their needs, the situation is not as comfortable as one would like it to be. To provide information assurance, a plethora of policies, procedures, and standards have emerged in the global market that claim to provide the required protection. Because absolute information security is practically impossible, according to Gene Spafford, professor of computer science at Purdue university (Hagen, Albrechtsen, & Hovden, 2008), and with all of these companies trying to "sell" their products, it is not easy for an organization to make the best choice. The CISO/CIO can choose from numerous international standards and guidelines that are available to implement in their organization. The proponents of each have their own arguments as to why a particular standard or guideline is better for an organization. The purpose of this chapter is to cut through all the jargon, get to the heart of enterprise security, and provide actionable information for establishing appropriate policies, procedures, and standards for enterprise-level security. In this chapter the authors have tried to sieve through the available options and organize them in a fashion that makes it easier to select the most appropriate components for their particular organization. This chapter outlines various major standards and approaches to information security.

Although it is essential to look at the available standards, yet, it is first fundamentally indispensable to understand the concept of enterprise-level information security and how these standards fit into its information security framework. Enterprise information security may be divided into three levels: strategic, tactical, and operational. Based on the classification by Johnson (2003), the information security policy is at the top. This is going to establish the information security stance of an enterprise and steer the whole information security effort. It should be aligned with the business strategy of the enterprise. At the tactical level, the information security policies might be used to define standards that can then be translated into procedures at the operational level.

Before we proceed much further, it would be a good idea to define the various information secu-