Chapter 1
A Framework for ICT Security Policy Management

Sitalakshmi Venkatraman
University of Ballarat, Australia

ABSTRACT

Organisations around the world are increasingly relying on the potential of information and communication technologies (ICTs) for their business operations as well as competitiveness. Huge amounts of money and time are invested on ICT infrastructure as there exists a high level of business dependency on ICT. Hence, protecting the ICT resources using effective security policies is of utmost importance for the sustenance of organisations. With the recent exponential rise in ICT security threats witnessed worldwide, governments and businesses are trying to successfully develop ICT security policies for their internal and external operations. While ICT security best practices are quite similar globally, ICT security policy management is very much localised and specific to different business scenarios and applications. Moreover, ICT security policies in an organization keep evolving from time to time and more recently changes take place at a much faster pace. This situation warrants a pragmatic framework for the development and management of ICT security policies in an organisation. Much research has focused on formulating frameworks for ICT management in general and there is a paucity of guidelines in literature for ICT security policy management, in particular. This chapter explores ICT security management issues faced in different environments and proposes an integrated framework for managing ICT security policies in an iterative manner. The framework provides the flexibility and adaptability for different organisations to follow the guidelines effectively as it emphasises on policy alignment with business objectives. Since the framework underpins the continuous improvement philosophy, it caters to ICT security policy reform and implementations for the future as well.

DOI: 10.4018/978-1-61692-012-8.ch001

INTRODUCTION

With information and communication technology (ICT) becoming part and parcel of business environments worldwide, the role of ICT security and its policies are of paramount importance in this globally inter-connected world (OECD, 2002; IT Governance Institute, 2005; Bojanc & Jerman-Blaic, 2008). Organisations, both private and public, have the critical objective of protecting their ICT infrastructure as well as business information assets from intrusions and risks (Conklin, 2007). Hence, it is mandatory for them to have in place suitable ICT security policies that could facilitate in achieving this objective.

Traditionally, before the onset of the Internet, ICT security policies were not given high priority among the various business strategies. Organisations were able to sustain with or without such policies. However, with the Internet explosion opening up global market opportunities, more and more businesses are harnessing the benefits of the inter-connectivity of ICT. Hence, formulating ICT security policies have become mandatory for the sustenance of every organisation (Caruso, 2003; Drevin, Kruger & Steyn, 2006). In addition, as shown in Figure 1, ICT security has become highly complex with three main dynamic changes taking place in the following areas that create new issues to focus on:

1. **Rapid ICT innovations:** new devices (mobile, wireless, etc) are getting inter-connected to traditional computing systems with different hardware and software platforms / protocols for businesses to operate on (Sathish Babu & Venkataram, 2009);
2. **Growing security threats:** recent security breaches are increasing exponentially creating a race between the hackers and the anti-virus solutions architects (Jahankani, Antonijevic & Walcott, 2008);
3. **Varying social and legal focus:** Globalisation requires business interaction between traditional and modern societies having different social and ethical beliefs / laws (Small, 2007).

Hence, ICT security policies have to be modified frequently to deal with the above said dynamic changes that impact both technological and non-technological areas. It is, therefore, important to incorporate security monitoring and planning steps that include protection measures, security standards, risk analysis and contingency plans so as to ensure information security in an organisation for the present as well as the future. All these steps require considerable effort, time and money and hence developing and managing an effective ICT security policy has become one of the main concerns for businesses worldwide.

This chapter aims to discuss the prevailing issues that face ICT security management and to propose an integrated framework for managing ICT security policies effectively. The main objectives of this chapter are:

- To explore the major issues and challenges that are surrounding ICT security policies,
- To understand the key global trends in developing and managing ICT security policies,
- To appreciate the need for a guideline towards ICT security policy management,
- To propose an effective framework for managing ICT security policies and for continuously reforming them,
- To understand the implementation details of the framework through the governance of ICT security policy at the strategic, tactical and operational levels of management, and
- To provide an overview of the future trends in the challenges, concerns and issues that organisations would face while managing their ICT security policies.