Chapter 25
Information Security Policies

J.R Ikoja-Odongo
Makerere University, Uganda

ABSTRACT

This chapter presents issues, trends, controversies and problems motivating organizations to establish information security policies or deter them from doing so. Its main thrust is to propose that organizations must take the issue of information security very seriously and provide solutions in their organizations. Information resources are a huge investment and the role information plays in any organization is no longer doubted. Increasing awareness of vulnerabilities to information resources is reason for information security policies. Policies provide opportunities to recognize the importance of procedures and mechanisms to enhance information security. Simultaneously avenues by which information may be compromised have increased many-fold. To counter the threats and risks and assure confidentiality, availability, accessibility, integrity, and authenticity of information, organizations draw up and set up information security policies.

INTRODUCTION

Literature on information security policies worldwide runs into millions of hits. According to Google, this literature runs to about two hundred fourteen million hits. This reveals that the subject of information security is a pressing issue of the present times. This chapter attempts to selectively refer to this literature to highlight the significance of this topic and to emphasize why organizations require to develop information security policies.

Information security policies are essential in the management of organizations. Many potentially damaging situations can be avoided or minimized by proactive planning and good management policies. The main objective of information security policies is to achieve three main objectives: confidentiality, integrity and availability of information (McLeod & Schell, 2007). Other aims are to achieve authenticity

DOI: 10.4018/978-1-61520-847-0.ch025

and privacy (Canavan, 2001) of information from both inside and outside the organization. Although total security of information is unattainable in any service organization, effort should be invested in preventing or deterring crime and curtail risks to which information is exposed (McDonald, 1994). It is one of the fundamental design principles of information security that information should be consistently protected according to its sensitivity, its criticality, and its value (Wood, 1996).

This chapter is intended to explain why security is important; gives an explanation and significance of information security policies to an both individuals and organization; describes the meaning of information security, threats, risks and policies; lists types of information security policies business entity can adopt or adapt; highlights the need for an information security policy in an organization; identifies sources of best practices in information security standards and policies; and suggests a framework for safeguarding information assets in organizations.

BACKGROUND

Worldwide, information and communication technologies (ICTs) have sparked a revolution in human history due to the rate at which these technologies are proliferating. Developments in ICT are fast. Rate of diffusion is equally exceptional. Uses to which they are deployed are diverse, for instance space science, artificial intelligence, and human genome studies. Their applications, especially with the emergence of the Internet and World Wide Web, have led to tremendous access to information. Surrounding this silver lining is the dark side. Computers are also now used for the design, proliferation and exploitation of weapons of mass destruction, military aircraft, nuclear submarines, biologic and chemical weapons, and reconnaissance satellites and space stations (Bosworth & Jacobson, 2002) as much as they are used for peaceful managerial and business purposes. The rapid entry and expansion of computers in the global economy; increased use on almost every continent and developments in computer networks are some of the reasons that have aroused security concerns (Ministerstvo, 2002).

Security concerns are rising because information has grown to be a significant economic resource with huge investments made on it. Unlike the brick and mortar days when, time was money, now information is money (Tuthill, 2001). Without information there is danger of an organization ceasing operations, failing to achieve competitive advantage, and finding difficulty in decision making and problem solving, because job performance is jeopardized and operating within the law can be difficult (Mutula & Wamukoya, 2007). Secondly, interest in information security matters has grown after many years of neglect. It is only in the recent times that management of institutions are appreciating that, as more systems are networked, the vulnerability to certain threats increases exponentially (Wood, 1996). Thirdly, the rise of electronic commerce has also heightened awareness among organizations of the information security threats, and fear of security breaches (Fulford & Doherty, 2003). Fourthly, widespread recognition that information now constitutes a "key corporate asset", which is of great commercial value has also brought information security nearer to the top of the management agenda (Gerber; Solms & Overbeck, 2001). To a large extent, such threats are growing because of higher levels of interconnectivity both within and between organizations (Dinnie, 1999; Barnard & von Solms, 1998). In such circumstances information security is no longer a domestic issue. In this age of electronic commerce, one company's information security certainly affects their business. This is because people get fully reliant on information technologies for managing their businesses in a way that proper information protection and proof thereof may be demanded at the standard practice by the business partners as the only way of doing business (von Solms, 1999). To mitigate these developments, organizations have and are developing information security policies.