Chapter 16
E-Business and Security

Sharon Nachtigal
Royal Holloway, University of London, UK

ABSTRACT

This chapter is concerned with a major problem for any e-business organization, the security of its Information Systems. A review of information security characteristics and components is presented, followed by a detailed discussion of e-business security issues. Based on a structured approach for describing e-business functionality, e-business characteristics relevant to information security are identified. The major e-business security challenges are considered and e-business security issues are discussed and requirements are identified in different aspects of the realm. The current perimeter security approach appears to be inadequate to the modern business environment. Hence, a different approach is needed. A few alternative approaches are discussed and a review of previous and future research on e-business security is presented. Hence, the chapter aims to contribute both to academics and to e-business executives by providing the information security insight and awareness to the e-business unique security issues and challenges.

INTRODUCTION

E-business has unique features, derived from its use of Information Technology. The definition identifies an e-business as a company running its business processes electronically (Nachtigal, 2007).

DOI: 10.4018/978-1-60960-501-8.ch016

Today’s organization faces a business environment which is very different from that of the 1980s; the possibility of interacting with suppliers, customers, competitors, partners, and financial and government institutions via the Internet changes the way operations are performed, the business and financial relationships, and the ways of dealing with money. As a result, there are new
security vulnerabilities and threats, and so this new environment requires a different set of security goals. Knowledge about secure e-business mode of doing business appears to be essential in order to implement it effectively.

BACKGROUND: INFORMATION SECURITY ISSUES

In this section the basic information security concepts and terms are presented. The presentation of the information security basics is essential in order to proceed with the unique e-business security challenges, which are discussed in the rest of this chapter.

The business environment is constantly changing along with (and due to the) advances in technology. Indeed, business environment benefits from advances in Information Technology (IT) by expanding and/or modifying its business activities, but also these advances in IT produce a new range of threats. A threat can be defined as any circumstance or event that has the potential to harm a system (Slade, 2006). The various threats to information and Information Systems (IS) also constantly change, depending on a specific business environment, IT environment, specific business goals and functionality. Hence, it is not possible to provide a list of all possible threats, but their classification into four categories (Bishop, 2005), such as:

1. disclosure (unauthorised access to information);
2. deception (acceptance of false data);
3. disruption (interruption or prevention of correct operation); and
4. usurpation (unauthorised control of some part of a system).

Although the level of information security varies according to specific threats relevant to a specific organisation, there are common general security goals. Confidentiality, Integrity, and Availability (CIA) are commonly considered to be the fundamental goals of IT security (Slade, 2006); they are sometimes also referred to as objectives, requirements, or properties (see, for example, (Furnell, 2005; Harris; Tettero, 2000)).

Sinclaire (2005) based his findings on a review of a range of MIS research literature published over the period 2002 - 2004 in four highly ranked journals¹ for IS research publications. The author makes a distinction between information security and information privacy. Based on the definitions of information privacy as the ability of the individual to control personal information about one’s self (Stone et al cited in Sinclaire, 2005), and the Panko (cited in Sinclaire, 2005) definition of IT security as providing confidentiality, integrity, and availability, Sinclaire (2005) presents the following statistics regarding research on security. A total of 24 articles were reviewed, of which 74% addressed information security and 26% addressed information privacy; 29% of the information security research articles address planning, and 71% address protection. Analysis of research within the protection category reveals that 50% pertain to authentication/verification, 25% are about types of threats, 17% address standards, and eight percent pertain to firewalls. Analysis of information privacy research reveals that 67% address user perceptions and the remaining 33% pertain to surveillance issues. In this context confidentiality refers to the holding of sensitive data in confidence, limiting access to an appropriate set of individuals (Slade, 2006).

Integrity involves maintaining the accuracy and reliability of information and systems, and preventing unauthorised modification of data, thereby ensuring that data is correct as defined by the process designer (Harris; Tettero, 2000).

Availability refers to the state when the system, resources, and data are in the place needed by the user, at the time the user needs them, and in the form the user needs (Slade, 2006).