A Management Perspective on Risk of Security Threats to Information Systems

FARIBORZ FARAHMAND  ff@cc.gatech.edu
SHAMKANT B. NAVATHE  sham@cc.gatech.edu
College of Computing, Georgia Institute of Technology, Atlanta, Georgia 30332-0280

GUNTER P. SHARP  gsharp@isye.gatech.edu
School of Industrial and Systems Engineering, Georgia Institute of Technology

PHILIP H. ENSLOW  enslow@cc.gatech.edu
College of Computing, Georgia Institute of Technology, Atlanta, Georgia 30332-0280

Abstract. Electronic commerce and the Internet have enabled businesses to reduce costs, attain greater market reach, and develop closer partner and customer relationships. However, using the Internet has led to new risks and concerns. This paper provides a management perspective on the issues confronting CIO’s and IT managers: it outlines the current state of the art for security in e-commerce, the important issues confronting managers, security enforcement measure/techniques, and potential threats and attacks. It develops a scheme for probabilistic evaluation of the impact of security threats with some illustrative examples. This methodology may be used to assess the probability of success of attacks on information assets in organizations, and to evaluate the expected damages of these attacks. The paper also outlines some possible remedies, suggested controls and countermeasures. Finally, it proposes the development of cost models which quantify damages of these attacks and the effort of confronting these attacks. The construction of one such cost model for security risk assessment is also outlined. It helps decision makers to select the appropriate choice of countermeasure(s) to minimize damages/losses due to security incidents. Finally, some recommendations for future work are provided to improve the management of security in organizations on the whole.

Keywords: business, cost, information system, management, security, threat

Introduction

The vast growth potential of Internet-based commerce is tempered by legitimate concerns over the security of a system that has a large number of potentially vulnerable components. Despite the potential rewards of conducting business on the Internet, some corporations have been slow to embrace this technology. Perhaps the most important reason for both businesses and consumers to refrain from establishing and participating in electronic commerce (e-commerce) is the potential for loss of assets and privacy due to potential security breaches in such systems. For example, a single, highly-publicized security breach can erode confidence in the business and not only damage the reputation of the firm, but can cause widespread repercussions in the e-commerce industry.
Commerce always involves payers and payees who exchange money for goods or services. Building trust between the payer and the payee on the Internet, intellectual property rights, and interactions between the payers and the payee are the new issues of commerce of our age. Security is essential in establishing this trust and interaction. These issues as well as some special considerations for the mobile e-commerce are addressed in the next part of this paper.

A very large amount of time and money has been spent to provide secure networks and many good practices have been developed to implement security measures. However, there is always the possibility of a breach of security. A list of possible attacks to the network, security measures at the database and network levels and some models for access control are presented in the Section 3 of the paper.

Regardless of all the existing countermeasures, statistics show that chances of computer security system failure are still very high. The Internet Fraud Complaint Center, IFCC (a partnership of the National White Collar Crime Center and the Federal Bureau of Investigators) reports 16,775 complaints of fraud for the Jan. 1, 2001–Dec. 31, 2001 period. The majority of these frauds were committed over the Internet or similar online services. These frauds have caused serious tangible and intangible losses to the companies and e-commerce industry as a whole. The authors believe that to have a systematic study of e-commerce security issues, we first need an organized classification that helps our understanding of threats. After highlighting the literature review on existing classifications, we propose a comprehensive classification for threats and countermeasures at the end of Section 4. Then we discuss the implications of security incidents, review some of the existing methods to quantify their costs, and propose a risk management system to evaluate the threats and countermeasures. We also provide some recommendations to assist managers in facing the challenges of e-commerce.

## 1. Electronic commerce security issues

The recent burgeoning of new communication technologies and, in particular, the Internet explosion has brought electronic commerce to the early stages of a widespread deployment. However, businesses are concerned about trading beyond this stage, largely because of concerns about trust, intellectual property management, and security of transactions, and possible attacks to the network.

### 1.1. Trust in electronic commerce

Traditional commerce is different from electronic commerce for several reasons: (1) In traditional businesses, the location of the business, the physical inventory of goods etc., is known. (2) In most of situations, there is a personal contact between the seller and the buyer, (3) There is a clear legal framework. Lack of these can highly impact trust in electronic commerce business. Several researchers have studied trust in electronic commerce.