Chapter 14
IT Security Governance in E-Banking

Theodosios Tsiakis
Alexandrian Technological Educational Institute of Thessaloniki, Greece

Theodoros Kargidis
Alexandrian Technological Educational Institute of Thessaloniki, Greece

Aristeidis Chatzipoulidis
University of Macedonia, Greece

ABSTRACT

Most industries have been influenced in different ways by e-commerce, and the banking industry is no exception. Particularly, banks are embracing electronic banking (e-banking) as a service to reach a wider market share, increase customer satisfaction and lower operational costs. This increased supply and demand in e-banking services has caused not only opportunities but also risks. The need to manage and regulate those risks calls for a sound Information Technology Security Governance (ITSG) program as means to deliver value business and mitigate Information Technology (IT) risks. In this regard, the chapter’s objectives are to explore, evaluate, and compare the current status and characteristics of Information Security Governance (ISG) approaches for e-banking. Therefore, the authors focus on an analysis of reputed best standards, guidelines on governance, risk management methods, and internal controls currently used for e-banking as means to research which satisfies best ISG objectives. Results show that banks should not be restricted to currently used approaches to ISG for e-banking but should take into consideration benefits and shortcomings other approaches possess. In this regard, the authors propose an ITSG framework for e-banking as a continuous process for assuring ISG objectives. They also highlight the importance of consistent measurement of metrics of ITSG performance with the aid of security content automation protocol.

INTRODUCTION

Since the beginning of modern network technology, especially the Internet, financial institutions have renovated their communication and business infrastructure in order to take benefit of advances in technology. It is evident that electronic banking (e-banking) has contributed substantially to the success and profitability of many banks (Kondabagil, 2007). Nevertheless, the parallel
expansion of digital attacks has made stakeholders lose confidence on e-banking operations (Gikandi and Bloor, 2010).

The evolution of e-banking has moved banking services from back-end applications to customer-centric network ends. Particularly, the open networked environment provides instant global access to information products and services so now the consumer can access the bank to conduct financial services instantly. Common e-banking services include but are not limited to financial information news, ATM (Automated Teller Machine) locators, insurance, credit cards, cash management, funds transfer, investment services and others (Baten and Kamil, 2010).

With society’s dependence on technology the risks as well as the failures to assure information has increased in a high rate. Particularly, the total amount of security breach and computer viruses cost globally $1.6 trillion a year and 39,363 human years of productivity for financial institutions (Symantec, 2010). Another incident in 2007 accused three cyber thieves for stealing $450,000 from the City National Bank in North Carolina (Vijayan, 2010) when recently in New Jersey, an attempt to steal information from more than 500,000 bank accounts got a bank employee arrested (MSNBC, 2010).

Banks ability to take advantage of the proliferation of technology often depends on open, accessible, available, and secure network services. Financial institutions depend on human notions such as customer trust, confidence, and satisfaction that appear to be the key indicators correlated to the growth of a business. As a result, retaining a good reputation for safeguarding information will increase market share and profit. In this respect, there is typically nothing that causes customer dissatisfaction more that compromised accounts or stolen identities, all purviews of security (Tan et al., 2010). For this reason and because banks should mitigate the information technology (IT) risks to an acceptable level, the concept of Information Technology Security Governance (ITSG) concept is tested as the main objective of this chapter under the prism of e-banking.

Particularly, we stress the importance for a financial institution to have a much more sophisticated and structured approach to ITSG as part of a wider Risk Management approach. In this regard, we focus on strengthening the relationship between Risk Management methods and ISG frameworks to approach the objectives of Security Governance in e-banking. Therefore, our main research objectives are to:

1. Empirically examine congruent terminology, role and implementation of ITSG in e-banking.
2. Research on e-banking risks with emphasis on outsourcing risk because it causes and affects other e-banking risks.
3. Focus on an overview of reputed approaches to ISG to meet the specific needs of e-banking systems.
4. Propose an ITSG framework for e-banking helping small banks achieve higher business value.

Just as new trends in information security (IS) require consistent measurement of metrics, we also consider how ITSG performance in e-banking can be measured. We summarize the chapter by supporting the argument that “Security is a management problem, not a technical problem” (Brotby, 2009, pp.15) especially in e-banking due to the interaction nature. This chapter is organized into ten sections. This section introduces the reader with the evolution of e-banking and main research concerns. Section two portrays the literature review of ITSG and e-banking in general and emphasizes on congruent terminology. Section three discusses the objectives of Information Security Governance (ISG) and most reputed approaches. Section four describes the role of ITSG in e-banking and proposes an ITSG framework as a basis for banks wishing to govern information security in the e-banking domain. Section five describes