Chapter 4.7
A Case Study of Effectively Implemented Information Systems Security Policy

Charla Griffy-Brown
Pepperdine University, USA

Mark W. S. Chun
Pepperdine University, USA

ABSTRACT

This chapter demonstrates the importance of a well-formulated and articulated information security policy by integrating best practices with a case analysis of a major Japanese multinational automotive manufacturer and the security lessons it learned in the implementation of its Web-based portal. The relationship between information security and business needs and the conflict that often results between the two are highlighted. The case also explores the complexities of balancing business expedience with long-term strategic technical architecture. The chapter provides insight and offers practical tools for effectively developing and implementing information security policies and procedures in contemporary business practice.

INTRODUCTION

John Fisherman, *chief information officer* (CIO) at Akamai Motor Corporation[1] (Akamai), was just beginning to breathe easy again, but he lacked time. Six months earlier, his division, the *Information Systems Division* (ISD), created and implemented a Web-based portal called FieldWeb to provide front-end access to Akamai and Genki[2] (the performance luxury division of Akamai Motor Corporation) dealership data and to increase the efficiency of the company's *dealership sales managers* (DSMs) by over 18.16%. Following this implementation, the ISD intended to imple-

ment the Web portal in seven other areas of the organization. The company's security concerns had been addressed, but Fisherman knew that dealing with information security was an ongoing process, not a destination. His goal was to ensure that policies, processes, and procedures were in place to ensure that Akamai remained secure.

In order to protect information assets, firms must first clearly articulate management's expectations regarding information system security and ethics. Documented policies are the foundation upon which security architecture is built. This chapter provides insight and practical tools for effectively developing and implementing information security policies and procedures in contemporary business practice. In order to demonstrate the real-world struggle with best practices, this chapter centers on a case study analysis of a Web-portal implementation at Akamai. This Web-portal implementation was the first time Akamai opened up its back-end systems to the risk of the Internet. Consequently, the company had to carefully consider how to proceed with its portal implementation and to proactively rethink its information security policies while undertaking this large-scale deployment. The end result was the design of a secure system and the implementation of a new learning process to proactively and continuously develop security system policies.

POLICY DEVELOPMENT DOESN'T HAVE TO BE PAINFUL

Conventional wisdom holds that designing and maintaining security policy often gets bogged down in a bureaucratic inefficiency and seemingly never-ending wrangling. Otherwise, such policy is a carefully guarded document preserved on the security officer's computer. Some firms adhere to what is often referred to as the unwritten "primordial network security policy" (Watchguard, 2004), which states, "Allow anyone in here to get out, for anything, but keep everyone out there from getting in here."

The reality is that developing and maintaining security policy does not need to be shrouded in such extreme secrecy. Furthermore, security policy does not have to be perfect. However, it should be consistently reviewed and refined given the ongoing changes in business technology and circumstance (Baskerville & Siponen, 2002; Hong, Chi, Chao, & Tang, 2003). Regardless of organization size, companies must have articulated security policies in order to remain competitive and secure (Siponen, 2000). This section briefly outlines a few simple steps for developing the first draft of a security policy. Subsequent sections will provide a bird's-eye view of the development of security policy in a real-world business case.

As defined by the *Computer Security Institute* (CSI) (http://www.gocsi.com) and the *Systems Administration and Networking Security Institute* (SANS), security policies should indicate "purpose, scope, a policy statement, standards, action, and responsibilities." Policies should be written simply and clearly to minimize the effort in maintaining them. It is wise initially to refine the "purpose, scope, and policy statement" section so that it will not need to be changed, whereas the "standards, action, and responsibility" sections often require periodic modification. Also important to keep in mind is that system-specific policies are generally written with a specific technology in mind (e.g., Windows 2000, Linux, Solaris, etc.). In contrast, program policies are broader in scope and generally apply industry standards, such as ISO 17799 (Kwok & Longley, 1999). For program policies, such industry guidelines provide a considerable head start in security policy development.

Security policies are first and foremost about people, not technology. A recent survey by Harris Interactive (Figure 1) showed that while 65% of workers recognize that employees pose the greatest security risk, more than a quarter of companies surveyed had no written policy. Furthermore,