Chapter V

Privacy Protection Through Security

Martine C. Ménard, Policy Research Initiative, Canada

Abstract

This chapter discusses how implementing network and computer security can protect privacy of Internet users. It argues that personal identifiable information is valuable to both clients and businesses alike, and therefore, both are responsible for securing privacy. They must understand the vulnerabilities, threats, and risks that they face, what information requires protection, and from whom. Businesses must also comprehend the business issues involved in securing data. Finally, security measures should be a strong mix of technological, physical, procedural, and logical measures where each measure is implemented in overlapping layers. Proposed solutions must be flexible, meet the objectives and businesses goals, and be revised on a regular basis. The author hopes that by understanding the proposed security solutions, readers will be able to implement steps to protect their privacy or client’s privacy.
Introduction

The popularity of the Internet with its many e-services available is bringing more people online who simply want to browse or use services such as online banking or online shopping anonymously. However, their privacy as an individual is at stake since a lot of information can be and is collected without their knowledge or consent. Much of the information collected is done stealthily through cookies, logs on visited Web sites, or through silent installation of viruses, spyware, and Trojan horses that are often obtained through e-mails, drive-by downloads, or legitimate downloaded files that are infected. Organizations such as department or retail stores, banks, government departments, or any businesses with online services, by offering savings or convenience to consumers in exchange for personal information, are in a position to collect much information about individuals. These processes infringe on privacy since they remove customers’ rights to be left alone and not be profiled, be free from surveillance, and have control of information they share. Furthermore, privacy is breached when customers do not know what is being collected about them, for how long it will be kept, the purposes of collection, and if it will be shared with third parties.

The term “hackers” can be used to describe both good and bad individuals. They use their programming, analytical, and problem solving skills to either denounce vulnerabilities, security issues and promote solutions or use their knowledge and vulnerabilities of systems for their own gain. Therefore, what distinguishes them is the intent and goal behind their actions. The Oxford dictionary supports this by defining hackers as:

1. programmers that use their skills for good, or
2. individuals who use computers to gain unauthorized access to computer networks. For the purpose of this chapter, hackers will be seen as individuals with bad or evil intentions that use their skills and computers for unauthorized, illegal, or criminal activity against people, organizations, other computers, or networks.

Organizations are also vulnerable to privacy issues because of their increased reliance on digital data and services. A security and privacy breach could anger customers and shareholders, make shares drop, remove competitive advantages, and threaten the organization’s existence. Organizations are even more at risks of being targeted since their information resources are more interesting. An attacker, gaining illegal access to their systems, will not only gain prominence from the hacking community, but could also gain knowledge of thousands of credit card numbers, usernames and passwords, and other important information to commit identity theft. Therefore, organizations need to put security safeguards in place to protect themselves from liabilities, protect shareholders investments, and assign accountability.

Both organizations and home users have a responsibility in protecting privacy. First, users must believe that their information is valuable, and they must act like it is. This includes implementing security measures and forfeiting conveniences or savings when the exchange is not right or equal. Organizations must also implement security measures
Related Content

Identifying Services in Procedural Programs for Migrating Legacy System to Service Oriented Architecture
[www.irma-international.org/chapter/identifying-services-procedural-programs-migrating/72553/](www.irma-international.org/chapter/identifying-services-procedural-programs-migrating/72553/)

Consumer Value of Context Aware and Location Based Mobile Services
[www.irma-international.org/chapter/consumer-value-context-aware-location/54965/](www.irma-international.org/chapter/consumer-value-context-aware-location/54965/)

[www.irma-international.org/chapter/holistic-investment-framework-cloud-computing/70136/](www.irma-international.org/chapter/holistic-investment-framework-cloud-computing/70136/)

Changes in CRM Approach: Refined Functional Blocks for Customer Creative Engagement in Services
[www.irma-international.org/article/changes-in-crm-approach/142871/](www.irma-international.org/article/changes-in-crm-approach/142871/)

An Approach for Intentional Modeling of Web Services Security Risk Assessment
[www.irma-international.org/chapter/approach-intentional-modeling-web-services/44052/](www.irma-international.org/chapter/approach-intentional-modeling-web-services/44052/)