Chapter 12
Regulatory and Policy Compliance with Regard to Identity Theft Prevention, Detection, and Response

Guillermo A. Francia III
Jacksonville State University, USA

Frances Shannon Hutchinson
Jacksonville State University, USA

ABSTRACT

The proliferation of the Internet has intensified the identity theft crisis. Recent surveys indicate staggering losses amounting to almost $50 billion incurred due to almost 9 million cases of identity theft losses. These startling and apparently persistent statistics have prompted the United States and other foreign governments to initiate strategic plans and to enact several regulations in order to curb the crisis. This chapter surveys national and international laws pertaining to identity theft. Further, it discusses regulatory and policy compliance in the field of information security as it relates to identity theft prevention, detection, and response policies or procedures. In order to comply with recently enacted security-focused legislations and to protect the private information of customers or other third-party members, it is important that institutions of all types establish appropriate policies and procedures for dealing with sensitive information.

INTRODUCTION

This chapter discusses regulatory and policy compliance in the field of information security as it relates to identity theft prevention, detection, and response policies or procedures. In order to comply with recently enacted security-focused legislations and to protect the private information of customers or other third-party members, it is important that institutions of all types establish appropriate policies and procedures for dealing with sensitive information. Listed here are certain laws which must be considered when developing identity theft related policies; guidelines for creating, implementing, and enforcing such policies are also cited.

Figure 1. Annual ID Theft Incidents
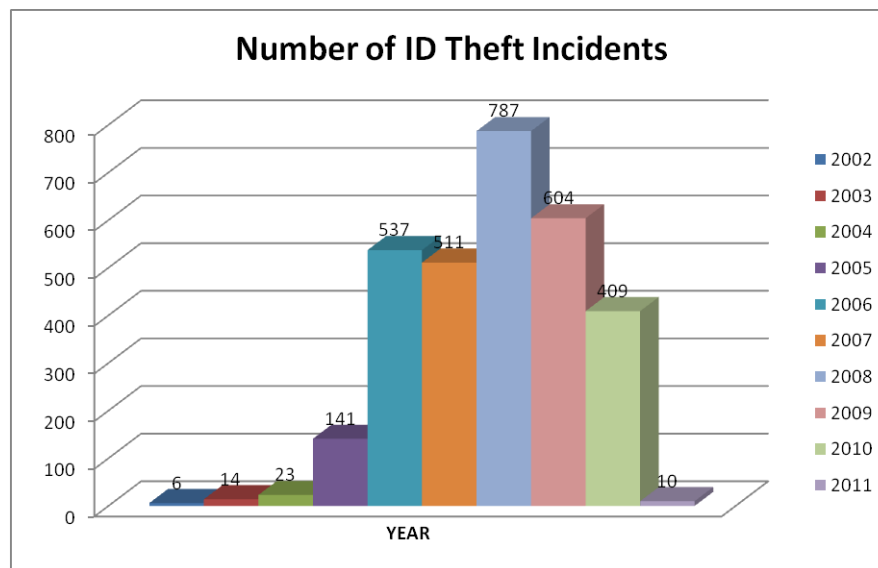
BACKGROUND

Identity theft is a threat that has confounded society since the biblical times. The ubiquity of the Internet and the convenience of electronic transactions have exacerbated the threat and made it even much easier to execute. Recent surveys indicate staggering losses amounting to almost $50 billion incurred due to almost 9 million cases of identity theft losses. A snapshot of several alarming statistics, which are gathered from the Open Security Foundation's DataLossDB (DataLossDB, 2011), pertinent to identity theft is shown in Figures 1 and 2. Figure 1 depicts the frequency of ID theft occurrences each year. As of February, 2011, there are already 10 incidents that involved ID theft.

Figure 2 shows the Personal Identifiable Information (PII) data loss categorized by data type in 2010. The data types are Date of Birth (DOB), Credit Card Number (CCN), Medical/Health information (MED), Social Security Number (SSN), Name and Address (NAA), and other miscellaneous information (MISC).

These startling statistics and their perceived persistent nature have prompted the federal gov-

ernment to initiate a strategic plan and several regulations to curb the crisis. We begin with the definition of important concepts pertaining to regulatory compliance and identity theft.

Definitions

Regulatory Compliance: A goal set by an organization in its attempt to comply with all laws or regulations relevant to that organization.

Policy Compliance: A goal set by an organization in its attempt to encourage and achieve compliance by its members/employees with regard to the organization's policies

Personally Identifiable Information: Any personal information by which an individual may be identified (SSN, bank account number, username/password combination, etc.).

Identity Theft: The co-option of another person's personal information without that person's knowledge and the fraudulent use of such knowledge (Princeton University, 2010)

Related Content

Network Security Software
Göran Pulkkis, Kaj J. Grahnand Peik Åström (2003). *Current Security Management & Ethical Issues of Information Technology (pp. 1-41).*
www.irma-international.org/chapter/network-security-software/7382

Information Security Governance and Standard Based Management Systems
Margareth Stolland Ruth Breu (2012). *Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions (pp. 261-282).*
www.irma-international.org/chapter/information-security-governance-standard-based/63094

A Comparative Survey on Cryptology-Based Methodologies
Allan Rwabutaza, Ming Yangand Nikolaos Bourbakis (2012). *International Journal of Information Security and Privacy (pp. 1-37).*
www.irma-international.org/article/comparative-survey-cryptology-based-methodologies/72722

Analysis of the European ICT Competence Frameworks
Luis Fernández Sanz, Josefa Gómez-Pérezand Ana Castillo-Martinez (2018). *Multidisciplinary Perspectives on Human Capital and Information Technology Professionals (pp. 225-245).*
www.irma-international.org/chapter/analysis-of-the-european-ict-competence-frameworks/198259

A SAT-Based Planning Approach for Finding Logical Attacks on Cryptographic Protocols
Noureddine Aribiand Yahia Lebbah (2020). *International Journal of Information Security and Privacy (pp. 1-21).*
www.irma-international.org/article/a-sat-based-planning-approach-for-finding-logical-attacks-on-cryptographic-protocols/262083