Chapter XXVI
Toward a Deeper Understanding of Personnel Anomaly Detection

Shuyuan Mary Ho
Syracuse University, USA

ABSTRACT

Recent threats to prominent organizations have greatly increased social awareness of the need for information security. Many measures have been designed and developed to guard against threats from outsider attacks. Technologies are commonly implemented to actively prohibit unauthorized connection and/or limit access to corporate internal resources; however, threats from insiders are even more subtle and complex. Personnel whom are inherently trusted have valuable internal corporate knowledge that could impact profits or organizational integrity. They are often a source of potential threat within the corporation, through leaking or damaging confidential and sensitive information—whether intentionally or unintentionally. Identifying and detecting anomalous personnel behavior and potential threats are concomitantly important. It can be done by observation and evaluation of communicated intentions and behavioral outcomes of the employee over time. While human observations are subject to fallibility and systems statistics are subject to false positives, personnel anomaly detection correlates observations on the change of personnel trustworthiness to provide for both corporate security and individual privacy. In this paper, insider threats are identified as one of the significant problems to corporate security. Some insightful discussions of personnel anomaly detection are provided, from both a social and a systems perspective.

ABSTRACT

Recent threats to prominent organizations have greatly increased social awareness of information security. Many countermeasures have been designed and developed to guard against threats from outsider attacks. Technologies are commonly implemented that will actively prohibit rogue connections or limit access to corporate internal resources; however, threats from insiders are even more subtle and complex. Personnel who also are trusted corporate assets generally have valuable internal corporate knowledge that could

impact profits. They are often the source of potential threats within the corporation, through leaking or damaging confidential and sensitive information—whether intentionally or unintentionally. Identifying and detecting anomalous personnel behavior and potential threats are concomitantly important. In this chapter, insider threats are identified as one of the significant problems in corporate security. Some insightful discussions of personnel anomaly detection are provided, from both a social and a systems perspective.

INTRODUCTION

The concept of information security and privacy have been discussed and researched in many disciplines. In the realm of political science, corporate ethics, secrecy, and sensitive information like the trade secrets, market competitive intelligence, and intellectual property are rigorously discussed. Corporate security policy that governs the principles of protecting corporate assets is therefore in place (Stevenson, 1980; Swann & Gill, 1993). Government surveillance of citizens for the sake of the national security has been a critical issue discussed throughout decades. George Orwell identified this issue in the book *Nineteen Eighty-Four*:

In the past, no government had the power to keep its citizens under constant surveillance. The invention of print, however, made it easier to manipulate public opinion, and the film and the radio carried the process further. With the development of television, and the technical advance which made it possible to receive and transmit simultaneously on the same instrument, private life came to an end. (Orwell, 1949, pp. 206-207)

Events surrounding the domestic surveillance scandal by the Bush administration (Associated Press, 2005) evolved as a result of expanding surveillance of terrorism activities into the lives of American citizens. The need for national security has begun to overshadow citizen's right to privacy. This principle applies to corporate governance as well. While government or corporate surveillance has terminated the freedom of personal privacy, the emphasis on personal privacy, however, would lead to a black box of human interactions within a corporate domain and, as a result, would threaten corporate, government, and national security. It becomes vitally important to balance individual privacy with surveillance interests governed by corporate security. How much security is necessary to protect corporate security interests, and how does this impact individual privacy? These questions are indeed a challenge today.

BACKGROUND

There have been ongoing discussions on the protection of business intelligence in order to remain competitive. Solutions in the social context can be found in business strategy, policy decisions, management processes, and in operational production. Social scientists have offered different aspects and findings in providing information assurance and security. Critical theory has been discussed and extensively applied in assessing management communication and interaction, accounting and information systems, as well as marketing and strategic management (Alvesson & Willmott, 1996). Social cognition has discussed the role of affect in cognitive-dissonance processes (Forgas, 2001). Whether a disgruntled employee could cause significant harm to corporate information security, how early such a negative impact could be detected, and how much change there would be on the trust level of an employee, and so forth are all critical issues to be studied. Furthermore, whether "the dark side of man" (Ghiglieri, 1999) would betray and change a person's trustworthiness after she or he has obtained high security clearance remains an issue. Incidents of such have been found on many occasions. Jonathan Pollard, for example, who had high-level security clearance, was arrested in 1985 for passing classified U.S. information, such as satellite photographs and weapon systems data, to Israelis (Noe, 2007; Haydon, 1999).