Cyber Insider Threat in Virtual Organizations

C

Shuyuan Mary Ho
Florida State University, USA

Jonathan M. Hollister
Florida State University, USA

INTRODUCTION

The concept of information security and privacy have been discussed and researched in many disciplines. In the realm of political science - corporate ethics, sensitive information such as trade secrets, market competitive intelligence, and intellectual property are rigorously discussed. As a result, corporate security policies are initiated and established to govern the principles of protecting corporate assets against potential risks, threats, and attacks. 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). Although our televisions don't provide two-way broadcast, the development of Internet provides a similar dynamic. Real world events surrounding the domestic surveillance scandal by the Bush Administration evolved as a result of redirecting surveillance of foreign terrorist activities into the lives of American citizens (Grey, 2005). The need for national security has begun to overshadow citizens' right to privacy. The case of Edward Snowden leaking sensitive information about the National Security Administration spying on United States citizens is a controversial case that frames Snowden as both a traitor and a patriot. Snowden intentionally stole and leaked information on the government's surveillance acts. This became a high-profile case of malicious intentional insider threat within the government (CNN Staff, 2013). But this phenomenon applies to corporate governance as well. While government or corporate surveillance may have superseded the right to personal privacy, the emphasis on personal privacy has led to a black box of human interactions within a corporate domain and, as a result, threatens corporate, government, and national security. It becomes vitally important to balance individual privacy with surveillance interests governed by corporate security policies. How much security is necessary to protect corporate security interests, and how much does this impact individual privacy? These questions are indeed a challenge today.

While the paradox of security and privacy persists, the problem of cyber insider threats becomes more complex due to the mobility of storage, communication media, and technology enabled by distributed, grid, and cloud computing. By definition, the virtual organization refers to a group of individuals whose members and resources may be dispersed geographically, but function as a coherent unit through the use of cyber-infrastructure. This group of individuals is team-based and goal-oriented, where leaders and subordinates work together to achieve pre-determined goals (Ho, 2009). Without the luxury of physical interactions or facial expressions, people collaborate with each other dynamically in virtual organizations using cyber infrastructure. To better discuss the "black box" of human interactions as supported by the computer-mediated technologies, we will first discuss the background information of organizations in regards to the availability of technology and variety of security procedures. We will then raise the issue of user problems in organizations, and further analyze the challenges of user problems in the social and digital domains of virtual organizations. We will discuss the challenges and possible future research

DOI: 10.4018/978-1-4666-5888-2.ch145

direction in analyzing user's deceptive information behavior in computer-mediated communications within virtual organizations.

BACKGROUND

Corporate espionage impedes organizations' integrity and competitiveness (Chan, 2003). Business intelligence is always an issue between competing profit-oriented corporations and organizations. In organizations and management studies, ongoing discussions ensue on how to protect business intelligence to remain competitive. Organizations have identified social and management approaches to re-focus their business strategies and policy decisions, and streamline processes and procedures in order to identify ramifications to secure information assets and ownerships. 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. Social cognition has discussed the role of affect in cognitive-dissonance processes. However, significant issues, such as when a disgruntled employee or systems' user would cause significant harm to corporate information security, how early such negative impacts could be detected and warned, and how would changes to security policies affect the trust level of an employee, remain under-studied. Furthermore, whether "the dark side of man" would cause a man to betray and influence their trustworthiness after s/he has obtained high security clearance remains elusive and ongoing issue. Such incidents have been found on many occasions. Johnson Pollard, for example, who had high-level security clearance, was arrested in 1985 for passing such classified U.S. information such as satellite photographs, weapon systems data to Israelis (Lamar, 1986; Noe, 2012). Chelsea Elizabeth Manning (formerly known as Bradley Edward Manning) on the other hand, posted Army's classified documents to WikiLeaks (McGreal, 2010), and was convicted for the violation of Espionage Act and sentenced 35 years (Tate, 2013).

These types of security incidents provide social context, and many of them are systematic and technical. These incidents range from physical facility breakdown, illegal network/system penetration, Internet transaction counterfeiting activity, to unauthorized modification or divulgence of confidential information. These incidents have raised the awareness of researchers and scientists to further investigate technical and systematic solutions for providing layered defense. Such awareness prompts us not only to identify vulnerabilities and threats in existing physical infrastructure, policy, operational procedure, personnel trustworthiness, and technologies, but also to investigate countermeasures and defense strategies in safeguarding both tangible and intangible assets. Many threats from malicious external hackers/crackers can be detected and prevented by both active and passive instruments[1]; however, threats from malicious personnel are generally more subtle and complex. The complexity and difficulty of identifying internal threats lies in the question of how much information and how much authority to entrust to those whom handle top secrets. The more knowledge a particular person has about internal resources, the greater the potential threat would be. Our ability to verify the trustworthiness of specific personnel becomes an increasingly critical and extensible research dimension in the area of personnel security.

Since critical information can be misused and the network can be spoofed either by outsiders or insiders, digital security[2] is implemented to prevent, detect, and protect corporate information assets. The systematic research perspective normally focuses on aggregating audit logs from selected resources (such as database, applications, and network devices) and builds individual uses behavioral profiles through natural language processing[3], text mining, and other information extraction techniques. The goal of these systematic detection approaches is to identify anomalies when compared to normalized information behavior patterns. However, in addition to digital approach, cognitive mapping and inference techniques are becoming important in learning about the corporate systems user's trustworthiness. Online games, for examples, can be designed and constructed in a way to allow simulation of a user's threatening or deceptive behavior scenarios to occur so as to afford a mechanism to study and inference future behavioral activities in social context. Rather than analyzing a user's digital logs from databases, network devices, or application time-stamps, the dyadic attribution model argues the fact that a user's language illustrating their intent and action can be evidence of information behavior, and proposes a mechanism to assess and infer trustworthi-