Chapter 6
The Ethics of Social Media and Network Security:
Issues in the Workplace

ABSTRACT

A definition of modern social media leads to the characterization of advantages and disadvantages of social media in the workplace. The characteristics of social media are: reach, accessibility, immediacy, and permanence paradox. The extent of media invasion of privacy is discussed in this chapter, and ethical dilemmas are raised. Social networks are regarded as the main reasons for the decrease of productivity and other unanticipated confidential problems, which a company may face. Furthermore, the implications of security alerts lead to a dilemma between individual privacy and common interest. Different types of attacks might interfere with an existing functional network. Relevant current issues in Network Security include: authentication, integrity, confidentiality, non-repudiation, and authorization.

INTRODUCTION

A social media site is a podium that permits user-generated content to emerge through interactions and associations in a virtual community. Security has several implications by which one must watch for. Heterogeneous networking technologies, higher speed connections, and ubiquitous access lead to theft of confidential information, unauthorized use of network bandwidth/computing resource, spread of false information, and disruption of legitimate service. Data diddling (the changing of data before or during entry into the computer system), spoofing, network eavesdropping, email related: virus, Trojan, worm.

BACKGROUND

Ever since the onset of the digital age, human reliance on computer technology and the Internet has grown and continue to grow exponentially. This growth, however, was constantly and consistently met with numerous security concerns. This is best

DOI: 10.4018/978-1-4666-7254-3.ch006

showcased by the fact that the "market for security software has witnessed an unprecedented growth in recent years" (Dey et al., 2012). As the name implies, providing Network Security is the act of monitoring activities being conducted in a certain network, and protecting the data being transmitted through the network from any form of outside or unwanted interference.

Network Security is the series of policies and provisions taken by a network administrator in order to ensure the safekeeping of a network and to prevent any possible unwanted or unauthorized access, alteration of data flowing through the network, and misuse or abuse of the network by individual who have access to it. The most basic form of network security, other than setting secure passwords for each individual using the network, is the firewall. The firewall could either be a software or a hardware-based security system that monitors the incoming and outgoing network traffic, and determines based on analyzing the information passing within the network whether data should be allowed through or not. There are two types of attacks that could compromise the security of a network: either passive attacks or active attacks (Wright & Harmening, 2009). Passive attacks include wiretapping, port scan, and idle scan. Active attacks are larger in number and most notable include denial-of-service-attack, spoofing, and format string attack (Wright & Harmening, 2009).

STATE OF THE ART

The security software market has witnessed a boom during the past few years. The number of individuals buying Network Security tools is increasing rapidly. In fact, this particular market has grown from 6.4 billion dollars in 2004, to 16.5 billion dollars in 2010 (Gartner, 2011). According to Dey et al., there are two main categories of Network Security software. These categories are:

1. **Off-the-Shelf Third-Party Standalone Tools:** Includes antivirus, antispyware, anti-spam-ware software among other products; and
2. **System Components:** Such as encryption software and firewalls that are engraved within the operating systems of computers.

There are currently 81 vendors of antivirus software in North America, and 87 vendors worldwide (Dey et al., 2012). The most prominent companies specializing in Network Security software are Symantec, McAfee, Kaspersky and others.

One type of vulnerabilities that unauthorized individuals could use to hack into a network is the open ports used in wireless networks. The frequency of usage of wireless networks is increasing rapidly, as a growing number of public places are using such networks to provide internet services to incoming clients. In fact, there was an estimated 143,700 public access points worldwide as of 2006, and this number was projected to increase to 818,700 throughout 2007 (Chenoweth et al., 2010). These public access points, also known as hotspots, are used in a wide array of establishments such as airports, coffee shops, restaurants, hotels, etc… These establishments are usually located in heavily populated areas, making the threat of network hacking through open ports very real. With more and more users getting accustomed to connecting their wireless devices to these freely available hotspots, the threat of these users picking up malicious codes that compromises their private information increases (Chenoweth et al., 2010). In 2010, Chenoweth et al. investigated the vulnerabilities present in public access points located on a college campus. Their data was collected during a period of 41 days. During this period, 3331 unique users accessed the public access points available on campus. The results of the study revealed that 8.62% of the 3331 computers that connected to the campus hotspots had an open