Combating Computer Fraud

Steve Brown
Capella University, USA

INTRODUCTION

Money is to be made with computer fraud. While this statement seems to be shocking, it is nonetheless a very real indication of the seriousness of the nature. As we are becoming more dependent on technology for our information and convenience, and the lack of process being made in stopping computer fraud, we are increasing the risk we place on ourselves. Computer fraud is often perpetuated by computer professionals who have an understanding of information technology. They have an advantage over the normal computer user, and due to the anonymous nature of the Internet, it is often difficult to catch and try suspects (Lynch, 2003).

What is still interesting is that corporate America is usually reluctant to bring criminal charges, even though Rommey (1995) reported that the average loss due to computer fraud was $109,000.00 and 90% of companies have reported they were a victim of computer fraud. Further, the Federal Bureau of Investigation has reported that reports of computer fraud have been declining (Hanna, 2005).

One of the main reasons Hanna (2005) and Rommey (1995) report on the decline of incident reporting is the possibility of bad publicity. During this span of 10 years, some of the reasons for not reporting incidents, that is, fear of bad publicity, remain the same. This could suggest that criminals are not worried about repercussions and feel the chances of getting caught are slim. Another reason might be that organizations are so dependent on their information systems that the main goal is simply to get back up online and in business (Cronan, Foltz, & Jones, 2006).

TYPES OF COMPUTER FRAUD

Organizations are under constant bombardment, and it is not uncommon for an organization to be attacked by "thousands of scans, probes, pings, and viruses" (Hanna, 2005, p. 34) on a daily basis. Computer fraud is not always a one-way attack; a newer type of attack called phishing, actually relies on the individual to initiate some action and give some information. According to the Anti-Phishing Working Group (APWG), 5% of individuals who receive an e-mail will respond with personal information; it is actually the victim helping the criminal. It can then be seen that the scope of this type of fraud is only limited by the size of the population the attacker wishes to contact (Knight, 2005).

Computer fraud can take on different activities; it can be internal or external. It can be employees stealing data, faking data entry input, management editing and/or altering financial information, or so-called fraudulent financial reporting where the National Commission on Fraudulent Financial Reporting (NCFFR) defines it as "intentional or reckless conduct, whether by act or omission, that results in materially misleading financial statement" (1987, p. 2).

Who commits computer fraud, and why would someone engage in this type of criminal activity? There are several possible reasons for this type of conduct. The term perpetrator is used to describe two sets of individuals, those who are authorized and those who are unauthorized users (Davis & Braun, 2004). Authorized users are those users who at one time have been granted access to a system for a legitimate purpose, where unauthorized users are those who neither have a legitimate purpose, or their authorized use was revoked. Davis and Braun (2004) reported that the largest group of perpetrators were those who were unauthorized users, but had somehow gained access, for example, breaking into a system. The motivation for authorized users was those who may have been laid off or terminated and used their authorizations to conduct criminal activity.

Some research suggests that it is people with low ethical standards that commit fraud (Ford, 1988). However, Cronan, Foltz, and Jones (2006) reported that in a survey of university students, 34% admitted to copying software. Does this mean that 34% of those who responded to the survey have low ethical standards, or are they simply not aware that copying software is considered a form of computer fraud? Corporate

espionage is also a possibility, Lenard (2005) reports on a case where an employee of one company was hired away by another company, but not before this employee was able to e-mail hundreds of important documents to his home account, where he was able to access them at a later time.

Computer fraud typically falls into one of several categories, which include:

- **Altering Input:** This is typically the simple process of altering data to show some change in quantity. For example, changing inventory levels so that it does not appear that inventory was in fact stolen. Altering data could also include the changing of someone's salaries, creating fictitious employees, and/or altering grade point averages for students (Rommey, 1995).
- **Copying Input:** This is the condition where computer data has been copied, for example, credit card numbers, social security numbers, and other personal or financial information was copied with a legitimate purpose (Davis & Braun, 2004).
- **Theft of Computer Time:** This involves using a computer for unauthorized processing. This would include the use of a company's computing system for other activities, like running a personal software program for his or her own purpose. This can lead to serious consequences, for example, if the system is needed for legitimate business purposes, or the unauthorized programs allows a malicious program to run that might be used later for further illegal activity (Rommey, 1995).
- **Software Modifications:** Modifying, deleting, and/or copying company software is a serious offense and costly to the organization. The Software Business Alliance, the trade group representing the commercial software groups, warns organizations that illegal copying of software can cost them in penalties from $150,000 to $250,000 per illegal copy (Rommey, 1995).
- **Phishing:** A social engineering attack, where e-mails and/or other correspondence directs users to Web sites, where individuals divulge some of their personal information, for example, banking information, user names, passwords, and so forth (Knight, 2005). A new form of phishing, termed vishing, is now taking place. Instead of e-mails, it is tricking individuals to offer up personal information by giving a user a telephone number to dial instead of visiting Web sites. E-mails and even personal phone calls direct unsuspecting individuals to a telephone number of the supposedly real financial institution. This is facilitated by the new Internet protocol voice over Internet protocol (VOIP) which allows criminals to quickly set-up telephone numbers from any area code, and set-up automated voice dialers duplicating a legitimate financial institutions' automated voice response system. These criminals will be gone, and the telephone number disconnected by the time the individual realized it was an attack (Hunt, 2006).
- **Pharming:** A new term is identified, or what Knight (2005) refers to, as "fishing without a lure" (p. 29). It is the use of a specialized hostile code, such as Trojans or key loggers, which copy an individual's keystrokes as he or she types. Poisoning is another type of pharming, where an individual believes they are surfing to a legitimate Web site, but end up at fraudulent Web site, offering up their valuable personal information.
- **Identity Theft:** Identity theft can be considered a form of pharming, where perpetrators use social engineering techniques and other forms of collection to obtain personal and financial information from individuals without their knowledge or consent. With identify theft, there are two victims: the individual, who must now try to repair the damage done to their credit rating; and the financial institution, where that information was stolen (Krause, 2006; Lynch, 2003). According to Lynch (2003), identity theft is one of the fastest growing crimes, and in 2002, it impacted at least 9.9 million Americans, and cost businesses $47.6 billion and consumers $5.0 billion.

COMPUTER FRAUD PROTECTION

Since computer fraud can have a huge financial impact, is it possible for organizations to put in place a comprehensive policy to eliminate, or at least reduce computer fraud? In the case of corporate or management fraud, some legislators and regulators believe that preventing fraud may be best done in the hands of auditors, and that in the normal course of their work, they are in the best position to detect fraud (Casabona & Yu, 1998). To also assist in this effort, the Auditing