1 Cyber Crime Defined

Employees of the organization commit most computer crime, and the crime occurs inside company walls (Hagen et al., 2008: Nykodym et al, 2005). However, in our perspective of financial crime introduced in this chapter, we will define computer crime as a profit-oriented crime rather than a damage-oriented crime, thereby excluding the traditional focus of dissatisfied and frustrated employees wanting to harm their own employers.

1.1 Computer Crime Technology

Computer crime is defined as any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation, or prosecution (Laudon and Laudon, 2010). The initial role of information and communication technology was to improve the efficiency and effectiveness of organizations. However, the quest of efficiency and effectiveness serves more obscure goals as fraudsters exploit the electronic dimension for personal profits. Computer crime is an overwhelming problem that has brought an array of new crime types (Picard, 2009). Examples of computer-related crimes include sabotage, software piracy, and stealing personal data (Pickett and Pickett, 2002).

In computer crime terminology, the term cracker is typically used to denote a hacker with a criminal intent. No one knows the magnitude of the computer crime problem – how many systems are invaded, how many people engage in the practice, or the total economic damage. According to Laudon and Laudon (2010), the most economically damaging kinds of computer crime are denial-of-service attacks, where customer orders might be rerouted to another supplier.

Eleven men in five countries carried out one of the worst data thefts for credit card fraud ever (Laudon and Laudon, 2010: 326):

> In early August 2008, U.S. federal prosecutors charged 11 men in five countries, including the United States, Ukraine, and China, with stealing more than 41 million credit and debit card numbers. This is now the biggest known theft of credit card numbers in history. The thieves focused on major retail chains such as OfficeMax, Barnes & Noble, BJ's Wholesale Club, the Sports Authority, and T.J. Marxx.
>
> The thieves drove around and scanned the wireless networks of these retailers to identify network vulnerabilities and then installed sniffer programs obtained from overseas collaborators. The sniffer programs tapped into the retailers' networks for processing credit cards, intercepting customers' debit and credit card numbers and PINs (personal identification numbers). The thieves then sent that information to computers in the Ukraine, Latvia, and the United States. They sold the credit card numbers online and imprinted other stolen numbers on the magnetic stripes of blank cards so they could withdraw thousands of dollars from ATM machines. Albert Gonzales of Miami was identified as a principal organizer of the ring.

> The conspirators began their largest theft in July 2005, when they identified a vulnerable network at a Marshall's department store in Miami and used it to install a sniffer program on the computers of the chain's parent company, TJX. They were able to access the central TJX database, which stored customer transactions for T.J. Marxx, Marshalls, HomeGoods, and A.J. Wright stores in the United States and Puerto Rico, and for Winners and HomeSense stores in Canada. Fifteen months later, TJX reported that the intruders had stolen records with up to 45 million credit and debit card numbers.
>
> TJX was still using the old Wired Equivalent Privacy (WEP) encryption system, which is relatively easy for hackers to crack. Other companies had switched to the more secure Wi-Fi Protected Access (WPA) standard with more complex encryption, but TJX did not make the change. An auditor later found that TJX had also neglected to install firewalls and data encryption on many of the computers using the wireless network, and did not properly install another layer of security software it had purchased. TJX acknowledged in a Securities and Exchange Commission filing that it transmitted credit card data to banks without encryption, violating credit card company guidelines.

Computer crime, often used synonymous with cyber crime, refers to any crime that involves a computer and a network, where the computer has played a part in the commission of a crime. Internet crime, as the third crime label, refers to criminal exploitation of the Internet. In our perspective of profit-oriented crime, crime is facilitated by computer networks or devices, where the primary target is not computer networks and devices, but rather independent of the computer network or device.

1.2 Computer Crime on the Internet

Cyber crime is a term used for attacks on the cyber security infrastructure of business organizations that can have several goals. One goal pursued by criminals is to gain unauthorized access to the target's sensitive information. Most businesses are vitally dependent on their proprietary information, including new product information, employment records, price lists and sales figures. According to Gallaher et al. (2008), an attacker may derive direct economic benefits from gaining access to and/or selling such information, or may inflict damage on an organization by impacting upon it. Once access has been attained, attackers can not only extract and use or sell confidential information, they can also modify or delete sensitive information, resulting in significant consequences for their targets.

Cyber crime is any crime committed over a computer network. Cyber crime is not limited to outside attacks. The most common type of cyber criminals, according to Nykodym et al. (2005), is occurring within their own walls. However, most of these crime types are innocent and petty. Examples include reading newspapers online, following sporting events while at work, or gambling online. Most of the perpetrators are between 30 and 35 years old. Some of the crime types are serious, for example theft. Persons over 35 years do the most damage.

Cyber crime and computer crime are both related to Internet crime. The Internet is a "double-edged sword" that provides many opportunities for individuals and organizations to develop. At the same time, the Internet has brought with it new opportunities to commit crime. Salifu (2008) argues that Internet crime has become a global issue that requires full cooperation and participation of both developing and developed countries at the international level.

Click fraud occurs when an individual or computer program fraudulently clicks on an online ad without any intention of learning more about the advertiser or making a purchase. When you click on an ad displayed by a search engine, the advertiser typically pays a fee for each click, which is supposed to direct potential buyers to its product. Click fraud has become a serious problem at Google and other web sites that feature pay-per-click online advertising. Some companies hire third parties (typically from low-wage countries) to fraudulently click on a competitor's ads to weaken them by driving up their marketing costs. Click fraud can also be perpetrated with software programs doing the clicking (Pickett and Pickett, 2002).

1.3 Financial Computer Crime

In this book, computer crime is classified as financial crime (Fletcher, 2007). Financial crime can be defined as crime against property, involving the unlawful conversion of property belonging to another to one's own personal use and benefit. Financial crime is sometimes labeled economic crime (Larsson, 2006). Financial crime is profit-driven crime to gain access to and control over property that belonged to someone else. Pickett and Pickett (2002) define financial crime as the use of deception for illegal gain, normally involving breach of trust, and some concealment of the true nature of the activities. They use the terms financial crime, white-collar crime, and fraud interchangeably.

The term financial crime expresses different concepts depending on the jurisdiction and the context. Nevertheless, Henning (2009) argues that financial crime generally describes a variety of crimes against property, involving the unlawful conversion of property belonging to another to one's own personal use and benefit, more often than not involving fraud but also bribery, corruption, money laundering, embezzlement, insider trading, tax violations, cyber attacks and the like. Criminal gain for personal benefit seems to be one of the core characteristics of financial crime.

Financial crime often involves fraud. Financial crime is carried out via check and credit card fraud, mortgage fraud, medical fraud, corporate fraud, bank account fraud, payment (point of sale) fraud, currency fraud, and health care fraud, and they involve acts such as insider trading, tax violations, kickbacks, embezzlement, identity theft, cyber attacks, money laundering, and social engineering. Embezzlement and theft of labor union property and falsification of union records used to facilitate or conceal such larcenies remain the most frequently prosecuted Labor-Management Reporting and Disclosure Act offences in the US (Toner, 2009).

Financial crime sometimes, but not always, involves criminal acts such as elder abuse, armed robbery, burglary, and even murder. Victims range from individuals to institutions, corporations, governments and entire economies.

Interpol (2009) argues that financial and high-tech crimes – currency counterfeiting, money laundering, intellectual property crime, payment card fraud, computer virus attacks and cyber-terrorism, for example – can affect all levels of society.

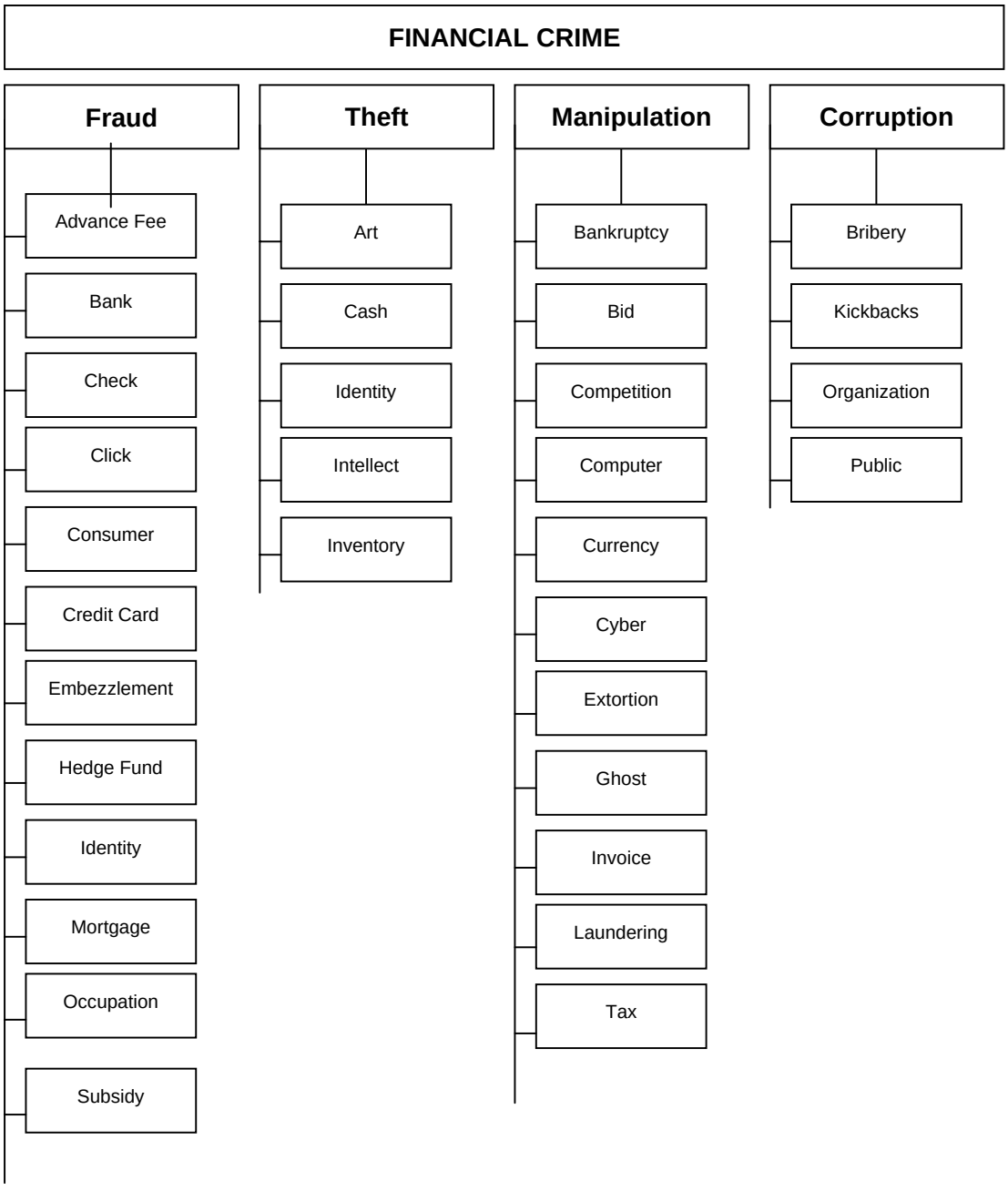

Figure 1. Main categories and sub categories of financial crime

We find a great variety of criminal activities that can be classified as financial crime. Figure 1 illustrates a structure among financial crime categories defined as main categories and sub categories of financial crime. The four main categories are labeled corruption, fraud, theft, and manipulation respectively. Within each main category there are a number of subcategories.

In Figure 1, computer crime is classified as a sub category of manipulation as a main category. Manipulation can be defined as a means of gaining illegal control or influence over others' activities, means and results. In addition to this direct kind of computer crime, we find indirect forms of computer crime, where computer technology is an important element of the crime. We have already mentioned examples such as identity fraud; click fraud, and credit card fraud that can be found under the main category of fraud in Figure 1.

By defining computer crime as financial crime and sometimes even as white-collar crime, as discussed below, we focus on the profit-orientation of such crime. This definition excludes incidents of computer crime to cause damage without a gain. Even if malware infection, hacking and other incidents are frequently reported in the popular press (Hagen et al., 2008), these kinds of computer crime are only of interest here if they have a profit motive. Computer crime is here profit-driven crime to gain access to and control over property that belonged to someone else.

Profit-driven crime by criminals should be understood mainly in economic rather than sociological or criminological terms. In an attempt to formulate a general *theory of profit-driven crime*, Naylor (2003) proposed a typology that shifts the focus from actors to actions by distinguishing between market crime, predatory crime, and commercial crime. The theory of profit-driven crime for white-collar crime suggests that financial crimes are opportunity driven, where executives and managers identify opportunities for illegal gain. Opportunity is a flexible characteristic of financial crime and varies depending on the type of criminals involved (Michel, 2008).

1.4 White-Collar Computer Crime

Computer crime can occur within white-collar crime, which is a special domain of financial crime. White-collar crime can be defined in terms of the offense, the offender or both. If white-collar crime is defined in terms of the offense, it means crime against property for personal or organizational gain. It is a property crime committed by non-physical means and by concealment or deception (Benson and Simpson, 2009). If white-collar crime is defined in terms of the offender, it means crime committed by upper class members of society for personal or organizational gain. It is individuals who are wealthy, highly educated, and socially connected, and they are typically employed by and in legitimate organizations (Hansen, 2009).

If white-collar crime is defined in terms of both perspectives, white-collar crime has the following characteristics:

- White-collar crime is crime against property for personal or organizational gain, which is committed by non-physical means and by concealment or deception. It is deceitful, it is intentional, it breaches trust, and it involves losses.
- White-collar criminals are individuals who are wealthy, highly educated, and socially connected, and they are typically employed by and in legitimate organization. They are persons of respectability and high social status who commit crime in the course of their occupation.

The most economically disadvantaged members of society are not the only ones committing crime. Members of the privileged socioeconomic class are also engaged in criminal behavior. The types of crime may differ from those of the lower classes, such as lawyers helping criminal clients launder their money, executives bribe public officials to achieve public contracts, or accountants manipulating balance sheet to avoid taxes. Another important difference between the two offenders is that the elite criminal is much less likely to be apprehended or punished due to his or her social status (Brightman, 2009).

Edwin Sutherland introduced the concept of "white-collar" crime in 1939. According to Brightman (2009), Sutherland's theory was controversial, particularly since many of the academicians in the audience fancied themselves as member so the upper echelon of American society. Despite his critics, Sutherland's theory of white-collar criminality served as the catalyst for an area of research that continues today.

In contrast to Sutherland, Brightman (2009) differs slightly regarding the definition of white-collar crime. While societal status may still determine access to wealth and property, he argues that the term white-collar crime should be broader in scope and include virtually any non-violent act committed for financial gain, regardless of one's social status. For example, access to technology, such as personal computers and the Internet, now allows individuals from all social classes to buy and sell stocks or engage in similar activities that were once the bastion of the financial elite.

Salifu (2008) provides support for our perspective of computer crime as profit-oriented crime, financial crime and sometimes even white-collar crime by arguing that economic reason lies at the heart of Internet crime. While there can be a number of motives, such as power, lust, revenge, adventure and the desire to check illegal boundaries and the likelihood of being caught, the most obvious motive is greed and profit. Far more computer crime is motivated by greed and the prospect of financial gain than any other motive.

White-collar crime represents a serious threat to corporate reputation. Nevertheless, there are surprisingly many corporations that are involved in white-collar crime. For example in Sweden, Alalehto (2010) found that 40 percent of the top-ranked corporations in the Swedish business world have been involved in white-collar crime in the last decade. These corporations had decisions against them, such as court decisions, administrative law, objection, or settlement.

1.5 Crime Offender or Victim

Most studies seem to apply the victim perspective of computer crime (Hagen et al., 2008). This perspective implies that an individual, a group, an organization or a society is the victim of crime. In this book, we will apply the offender perspective as well. The offender perspective implies that an individual, a group, an organization or a society is the criminal responsible for computer crime.

In the victim perspective, a survey revealed that next to malware infection and theft of IT equipment, hacking was the most commonly reported computer crime incident. The findings of Hagen et al. (2008) document that computer crime cause extra work for the victim and loss of earnings as well. Several of the reported crime incidents in their study could be countered by improved access control and data protection measures in addition to awareness raising activities. Their survey revealed that there are large differences in security practices between large and small enterprises, even when it comes to measures one might have thought that all enterprises independent of size would have implemented.