Objectives

after completing this lesson, you will be able to

» Understand what constitutes **computer crime;**

» Discuss the *history of computer crime,* including phone phreaking and hacking;

» Discuss *how criminals use computers* in embezzlement, theft, and espionage; and

» Discuss *how computer crimes can be prevented and controlled.*

For this lesson, please read:

» Rosoff, Pontell and Tillman, *White-collar Crime*:

- **Chapter 12. Computer Crime**

Computer crime is the fastest growing general category of crime in the United States. Not all of it comprises ***"white-collar crime"*** as it is usually considered, but much of it does involve major economic crime.

"

Computer crime has been described broadly as ***"the destruction, theft, or unauthorized or illegal use, modification, or copying of information, programs, services, equipment, or communications networks."***

"

A less formal definition is, **"Any intentional act associated with computers in which a victim suffers a loss and a perpetrator makes a gain."**

Generic computer-related offenses include the following:

- Electronic embezzlement and financial theft.
- Computer hacking and malicious sabotage, including the creation, installation, or dissemination of computer viruses.
- Utilization of computers and computer networks for purposes of espionage.
- The use of electronic devices and computer codes for making unauthorized long-distance telephone calls.

Computer crime has come a long way in a short time.

***The prevalence and cost of computer crime is almost impossible to calculate**, but by all accounts the figures are large and growing.*

- In 1986, one survey found that 7% of companies reported being victimized by computer crimes.
- By 1993, 70% of 400 surveyed companies reported at least one security violation in the previous 12 months, and 24% put the loss per incident at more than $100,000.
- In 1995, a university study showed that 148 out of 150 large companies surveyed reported victimization — 43% said they had been victimized 25 times or more.

Today, cost estimates range from $550 million to $15 billion internationally, depending on which acts are included as ***"computer crimes."*** Using current definitions, almost all business crime in the 21st century could be classified as computer crime.

> ***Moreover, if one includes the growing problem of software piracy as yet another form of computer crime, cost estimates climb even higher.***

There may be little agreement on the actual cost of ***computer crime***, but thus far no one questions that the losses are enormous.

For obvious reasons, computer crime has a rather short history.

> *The invention of the "blue box" in the early 1960s made it possible to duplicate the new frequencies used by AT&T for telephone dialing. The new technology was openly described in the telephone company's technical journals.*

Clearly, **AT&T** clearly did not yet recognize the first law of electronic crime: ***"If it can be done, someone will do it."*** The first phone phreaks gained unauthorized access to the entire telephone network and were able to make free calls around the world. **They were the first computer criminals.**

At about the same time, **computer technology graduated from enormous self-contained mainframes to interactive systems and primitive networks**.

Hackers began gaining unauthorized access to computers in the 1970s. **By the 1980s, when computers had become more common and were linked by modems, hackers found it even easier to break into computer systems.**

"

This initial mischief has given way to full-blown white-collar crimes of today.

"

» Hacking has been a mainstay of discussions about computer crime. Indeed, much computer crime could not take place without the skills and knowledge necessary to break and change codes, and gain unauthorized access to systems and files. **Numerous hacking cases are discussed at length in the reading.**

> ✱ ***The mischievous hackers of the early days of computing have given way to the larcenous criminals of today. The same skills are now being used to commit major crimes.***

» Playpen hackers, showoffs, and cookbook hackers have evolved into more malicious types such as the “stunt hacker,” who is out to do real harm. **Observers have found that many hackers appear to be egomaniacs looking for “respect” for their “talents.”**

» Rival hacker gangs in some ways mimic street gangs. **MOD (alternately known as the Masters of Destruction and the Masters of Deception) and the Legion of Doom are perhaps the most widely recognized gangs within the hacking subculture.**

* ***Moreover, the hacker subculture is a "meritocracy." Hackers receive more status based upon information they supply to other hackers.***

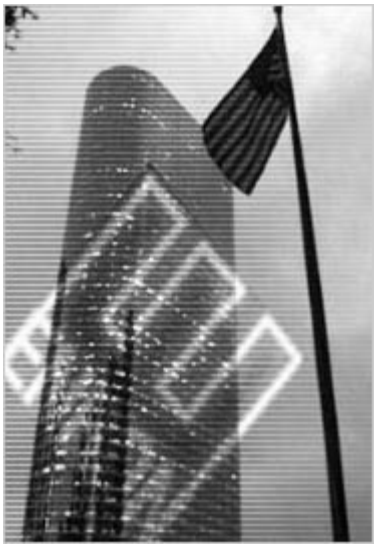
» **Hacking represents dangers to security, including issues of privacy, copyright violation, piracy, theft, and espionage**. They present additional dangers when they plant destructive computer viruses that quickly spread to computers worldwide.

Forum *discussion*

"to post your reply, select OUTLINE from the TOOLS menu and enter the FORUMS area"

Clearly, hacking is a major problem. With what you have learned from this course and others, what would you recommend in terms of its control and prevention. ***Why?***

» Write about two paragraphs on this question.



» It has been reported that the average US bank robbery nets approximately ***$3,177.70***. In contrast, it is estimated that the average computer crime may be as high as ***$500,000***.

"

Moreover, it could be said that ***computers have done for embezzlement what the microwave did for popcorn****. That is, made it extremely easy to do.*

"

Most reported cases of electronic theft take place from within companies and organizations, and involve insiders. It has become a maxim that the easiest way into a computer is usually through the ***"front door."***

> ***Much evidence also exists to support the idea that electronic embezzlers are found not only in banks, but in almost any private or public organization.***

The techniques for committing these crimes include a variety of programming tricks to divert funds. Among the most popular are:

- Entering false information (fictitious accounts and individuals, for example);
- Inserting a Trojan Horse or a “bad” program within a legitimate one that eventually diverts cash into fraudulent accounts; and
- Using trapdoors or sleepers that allow bypassing of security safeguards (“salami slicing” is a common form, where small amounts of unaccounted funds are siphoned off into phony accounts).

> *Such embezzlement becomes theft when similar techniques are used by someone outside the organization in question.*

Computer espionage has three major forms: **industrial, political, and international.**

Industrial espionage was reported to have increased ***260% between 1985 and 1993.***

*

It has also been discovered that computers have been used to obtain confidential information on political figures in order to damage their reputations.

International espionage is the most difficult to assess. The covert nature of spying hides many incidents, which can involve classified and secret documents.

> ***One thing is certain, however. As technology and accompanying equipment become more sophisticated, the threat of computer espionage becomes more serious throughout the world.***

In fact, phone phreaking — the oldest and most durable form of electronic crime — has moved into this area. Today, phone phreaks can do more than make free calls (called ***toll fraud***). **They can also tamper with financial accounts, and intercept and monitor other calls.**

"

*It has been estimated that toll fraud costs over $4 billion annually. The cost is passed on to consumers in the form of a covert "**fraud tax**" by victimized companies. Common toll fraud schemes involve "**call-sell operators**" who buy stolen access codes (from hackers or "**shoulder surfers**") and use them to make or sell long-distance calls.*

"

Phone phreaks have also moved into the area of industrial espionage, intercepting fax machine transmissions.

» Viruses, worms, and denial of service attacks (see readings) have all been responsible for causing major economic losses around the world. **Controlling these and other computer crimes is certainly one of the biggest challenges to law enforcement today.**

We can expect that controlling computer crimes will also be a major challenge in the future. Police agencies struggle to get up to speed and keep up with burgeoning technology that usually allows the smartest crooks to easily keep one step ahead of slower moving bureaucracies.

» As one seasoned FBI agent noted at a major computer crime conference held at the Bureau's training academy, **"There's Internet time, and there's government time."**

Recently, these issues have gained even more importance: ***Terrorists also use computers***. The threat of cyber-terrorism has grown dramatically. This form of computer crime can potentially cause much more damage and loss of life than any physical attack they might muster.

In any discussion about controlling computer crime, we should consider the following:

- Developing antifraud systems aimed at user-identification.
- Improving biometric technology (retinal scanners, DNA identification, handprint readers, and the like).
- Constantly upgrading and developing highly sophisticated “firewall” software designed to shield information and systems from hackers and thieves.
- Providing military style internal security measures with multiple control systems and continuous updating, and checking.

Perhaps the most important item to consider is this: ***Computer criminals respond consistently to improved security technology with improved criminal technology***. This makes it all the more important to never be comfortable with existing security systems for very long.

*

Summary

a brief overview of what you learned

» Computer crime is the fastest growing general category of crime in the United States. Generic computer-related offenses include electronic embezzlement and financial theft; computer hacking and malicious sabotage; utilization of computers and computer networks for purposes of espionage; and the use of electronic devices and computer codes for making unauthorized long-distance telephone calls.

» Today, cost estimates range from $550 million to $15 billion internationally, depending on which acts are included as "computer crimes." Using current definitions, almost all business crime in the 21st century could be classified as computer crime.

» Most reported cases of electronic theft take place from within companies and organizations, and involve insiders. It has become a maxim that the easiest way into a computer is usually through the **"front door."** A variety of programming tricks are used to divert funds.

» Computer espionage has three major forms: **industrial, political, and international**. As technology and accompanying equipment become more sophisticated, the threat of computer espionage becomes more serious throughout the world.

Objectives

after completing this lesson, you will be able to

» Be aware of the **complexity of the causes and cures** for white-collar crime;

» Understand that controlling *white-collar crime is one of our most important challenges*; and

» Discuss the *political, institutional, and societal changes* that are required in order to control white-collar crime.

For this lesson, please read:

» Rosoff, Pontell and Tillman, *White-collar Crime*:

- **Chapter 13. Conclusions**

» Pontell and Shichor, *Contemporary Issues in Crime and Criminal Justice:*

- **Short, "Technology, Risk Analysis and the Challenge of Social Control"**
- **Grabosky, "The System of Corporate Crime Control"**

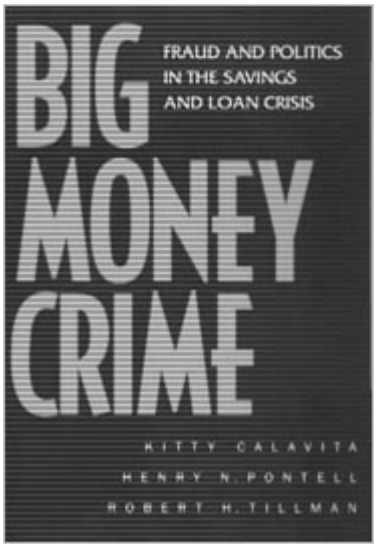
We have covered a lot in our relatively brief journey through the world of ***white-collar crime***.

"

As with most crimes, the causes and cures for this phenomenon are not simply stated. On the contrary: ***They are quite complex.***

"

In addition, ***white-collar crime*** in many instances appears to negate many common explanations of crime. It often flies in the face of common sense and our usual expectations.



*

In other words, when we see successful business enterprises and persons engaging in acts that clearly would jeopardize that success, our first reaction may be disbelief. But this happens time and again, which makes the field of white-collar crime that much more interesting to many who study it. And it also illustrates the fact that causes and cures are complex.

*

Professional violations may require more policing from within such groups, while widespread financial scandals clearly have more to do with regulatory structures and laws. **The culture of greed that sometimes dominates the social landscape can also influence behaviors in a number of ways, not the least of which is to help individuals neutralize formal social rules and norms that would otherwise provide effective controls on their behavior.**

» These cultural values in themselves, however, do not address structural issues that exist among individuals and within the context of societies, institutions, and organizations.

In examining specific forms of ***white-collar crime****, one must consider these elements, sometimes in combination. Some theoretical perspectives may be more salient than others, depending upon the case and the type of crime.*

The causes of ***white-collar crime*** can thus be examined at individual, societal, institutional, and organizational levels, as we have seen throughout the course.

* ***As noted in the readings, the concept of sociopathic wealth may go a long way in explaining the recent major waves of fraud that have swept the country and caused unparalleled levels of damage not only to the overall economy, but to individuals as well.***

  As also noted, not all organizational deviance conforms to a ***"greedy leader"*** model. In some cases the strain placed on a company by its organizational environment may also lead it into lawbreaking.

One of the most interesting and brighter aspects of ***white-collar crime*** is this: **Given the seemingly abundant opportunities for engaging in it, most persons choose not to.**

> *Many perhaps fear punishment (a deterrent effect), while others may simply not contemplate such acts at all due to their own moral compass. Some may not cheat on their taxes, for example, because of a sanction threat, but overall it seems that the risk-reward ration is out of balance when it comes to* ***white-collar crime****.*

That is, in most cases, the potential rewards greatly outweigh the risk. Given the relatively low probability of apprehension along with the likelihood of light punishment, ***white-collar crime*** appears to be a "rational" course of action in many cases.

Controlling White-Collar Crime

As we have also seen, the costs of ***white-collar crime*** — to the government and taxpayers, the environment, the economy, and society — are quite large. **The damage to fundamental institutions, while sometimes largely ignored compared to direct fiscal and human costs, is quite significant.**

"

In this regard, the connection between ***white-collar crime*** *and common crime is both direct and indirect. That is,* ***"crime in the suites"*** *and* ***"crime in the streets"*** *can feed off of each other in many ways.* ***White-collar criminality*** *can certainly facilitate other types of crime by promoting cynicism and resentment amongst the citizenry. In some cases it may even directly support illegal industries such as the drug trade — through money laundering, for example.*

"

"

For all of these reasons, controlling ***white-collar crime*** *is one of our most important challenges. Legal changes are necessary that configure regulatory systems and criminal statutes in a way that lowers rewards and promotes voluntary compliance. It should be obvious to even the most ardent* ***"law and order"*** *types that trying to control* ***white-collar crime*** *strictly through criminal statutes is destined to failure given the inherent power and resources of those who would stand accused, be they individuals or large corporations.*

"

Institutional changes are also necessary that pinpoint the sources of criminogenic industries and environments that foster illegality. Successful prevention strategies will attempt to "deinstitutionalize" ***white-collar crime***, or in other words, remove its institutional sources.

*

"Beating the competition" must be tuned to a morality that purportedly sees "playing by the rules" as an important virtue to be instilled in future generations.

*

Social changes are also necessary that have a variety of forms. Changing attitudes toward the phenomenon is necessary to allow for deserved stigmatization rather than a cynical **"respect"** for those who are clever or bold enough to fleece others out of millions of dollars.

The ethics of business may require considerable reworking, especially in business schools, where the captains of industry are trained. **Even the most elite educational institutions are severely lacking in this regard, which certainly means that those ranked below them cannot be any better, and likely much worse.**

Given these complex problems regarding the prevention and control of ***white-collar crime****, the incredible costs associated with it, and the number of fronts from which it needs to be addressed, perhaps the best starting point for change may simply be letting policy makers know — in no uncertain terms — that we care.*

Forum *discussion*

"to post your reply, select OUTLINE from the TOOLS menu and enter the FORUMS area"

Discuss the Grabosky and Short articles in relationship to their strengths and weaknesses for controlling ***white-collar crime.***

» Please post a few paragraphs on this topic.

Summary

a brief overview of what you learned

» In examining specific forms of ***white-collar crime***, one must consider these many elements, sometimes in combination. **Some theoretical perspectives may be more salient than others, depending upon the case and the type of crime.**

» One of the most interesting and brighter aspects of ***white-collar crime*** is this: **Given the seemingly abundant opportunities for engaging in it, most persons choose not to.**

» In most cases, the potential rewards of ***white-collar crime*** greatly outweigh the risks. Given the relatively low probability of apprehension along with the likelihood of light punishment, white-collar crime may appear to be a **"rational"** course of action.

» Controlling ***white-collar crime*** is one of our most important challenges. Legal, institutional, and social changes are all required in order to do this. **Perhaps the best starting point for change may simply be letting policy makers know — in no uncertain terms — that we care.**