Assignment Title

Student’s Name

Institutional Affiliation
Chapter 4

1. What is software piracy? How pervasive is it, and how can it be eliminated?

Software piracy is a phrase regularly used to define copying or using software in infringement of its license (commonly referred to as an end consumer licensing agreement). Software piracy is as widespread as the Internet itself. Nearly, 57 percent of computer users in the world say they are applying the unlicensed software. That contains 31% users that do it every day; and another 26 percent that admit pirating only seldom. These shocking findings have been derived from the survey of the Business Software Alliance organization. It contains approximately 15,000 PC users in 33 countries building up 82 percent of the worldwide PC market.

Software owners have developed a number of approaches to eliminate the so-called software piracy. Such techniques contain publicity about the damage that it supposedly causes, sudden audits of companies requiring users to connect with a vendor to get an installation code, a legal action, and selling the less expensive versions with less functions and the electronic copy protection.

2. How do contemporary hackers vary from their predecessors?

Nowadays, the hackers’ activity radically varies from before. First of all, the notion Script Kiddies has appeared. It refers to people basically using some "point-n-click" tools that endanger systems without actually knowing what is going on. Forerunner hackers have been extremely qualified and known the inner working of security mechanisms. Moreover, penetration required a lot more experience.

Formerly, the core motivation was to show the awareness and skills to a narrow audience. Rarely, there was an aim to cause harm and wreak chaos. Nevertheless, this situation has turned to the worse. Hacker’s penetration made today is done with the financial gain as a motivation. Moreover, there are new organized crime rings which act solely in the Internet domain, setting up botnets, and selling their services, etc.
3. Discuss six classifications of motivation for the contemporary computer intruders.

There are six primary elements of motivation classified for computer intruders. They are: boredom (informational voyeurism), intellectual challenge (mining for knowledge, i.e. pure hackers), revenge (insiders, disgruntled employees, etc.), sexual gratification (stalking, harassment, etc.), economic (such as criminals) and political one (terrorists, spies, etc.). The least destructive, but not less insidious, is a category of hackers that are considered to be as data voyeurs. Their motivation spans from curiosity to boasting and sensationalism. Luckily for the people’s security, these individuals are the easiest to be identified as they share their own slang, lifestyles and ethics. As a rule, these hackers have proclaimed themselves to be the seekers of data. Such hackers think they have some moral obligations to report of the protection holes to system administrators. However, they decline any individual who uses the knowledge for nefarious purposes.

Possibly, the most dangerous individuals to the information system security are ongoing and former employees, or the so-called “insiders”. Insiders have a valid access to the computer information, but have surpassed that authorization. Some insiders outflank security measures for their personal or financial greed. Thus, a major threat is posed by individuals that do this occasionally. In such a way, many more violations of the institutional security come from some inaccurate log-in practices than do any intentional attacks. Employees, posting the passwords in obvious places, allow others to shoulder surf using some unified names for passwords or spilling them to strangers. Thus, they cause a greater risk to the information security.

Further, the last two types of hackers are not quite spread as those previous intruders mentioned above. Their cases appear to be investigated at a higher rate. Hackers in these categories are interested for the personal or political greed. Criminals using the information technology to breach some traditional illegal statutes for their personal gain are appearing fast. Illegal hacking may be targeted at the information which has some values on its face or directed at the data which may be used to other criminal action for further.
4. What does the term "theft of information" mean? Discuss the implications of such in terms of the national security.

Theft of data is always a pointer of intention to use that information. There is no legal reason for an individual unaffiliated with the organization to access that organization’s sensitive data. Thus, the discovered compromise may be treated as a precursor of a future threat. Technology has also escalated the potential for some sophisticated attacks at the country’s national security. Unfortunately, government entities have not invested necessary resources to protect their secrets technologically saved or created. There appears to be no such apathy on the part of foreign governments. Indeed, the FBI estimates that at least 120 overseas governments are actively working over intelligence operations currently targeting at the US. On the other hand, the United States has seen the growth in trusted government agents accused of espionage. These threats are not only real, but are also increasingly complicated. In fact, a simpler and more widespread method of the technological theft involves physical robbery of information storage containers. The usage of laptop computers was heralded as the solution to the employee angst. Designed to trigger home-based work, laptops were intended to empower overburdened workers, enabling them to work at home, during their vacation or elsewhere. However, their introduction has not been accomplished without a row of associated problems. Practically, their sheer portability, seen as their greatest strength, is also their greatest weakness. In fact, it makes them the prime targets for burgeoning of the data black market. Unfortunately, a variety of laptops has been stolen recently, usually as a result of the employees’ carelessness.

5. How has technology changed the face of terrorism? How could it be utilized in the future?

Terrorism has existed for a long time and continues to be an actual danger in the today’s life. Technology notably has made terrorism more tempting to dissenters’ groups and ruleless states. In terms of globalization, new telecommunications ensure the online coverage of terrorist attacks, whether this happens in New York, Buenos Aires or Beirut. As we have moved into the 21st century, the new and even more powerful communication technologies will give terrorism a
greater power and appeal. Web terrorism is the newest technique that terrorists use to impose their acts of brute and dread intimidation for their targeted victims. And it is increasing as more terrorists discover the Internet as an accessible tool to communicate and plan their terroristic acts. Internet has provided terrorists with other method to perform an act of terror and reach a bigger amount of people. It also gives terrorists a chance to pinpoint the precise targets without even having to set their foot on the soil of this region they are aiming at. No longer a terrorist appears face-to-face or incites using bombs or brutes. With the governmental, economic and social connection to the web, an act of terror using Internet has the potential to extend the wrath of damage to reach millions of people by bringing down the complete infrastructures. This has a straight impact on many victims that could be thousands of miles away. Technology has significantly changed the face of terrorism. Now, the perpetrators of violence do not need to transfer to their target destinations. Cyber terrorism is a very real concern and safety issue in the today's world. In future, the entire banking, power plant, emergency service, telecommunications, military or government systems can bring a victim to a successful cyber terroristic attack. This could bear down the heart of an economy or state, as whole. Even if one object of this list has been cyber attacked it would cause a mass disorder and panic. In some cases, it may become even worse as it may result into a serious damage or death. In addition, terrorists are using technology as a weapon with the potential to be very dangerous which can outcome in a mass destruction.

6. Discuss the evolution of criminal behavior in the United States. Include in your answer the utilization of technological advances.

Many studies have suggested that the list of computer crimes in the U.S.A. alone is the millions; while others indicate that the cost to the state is in excess of several billion dollars. Nevertheless, hacking is an international problem not restricted to the US. Hackers have set up virtually in every state in which computer technology is being available. Notably, these individuals, irrespectively of their national origin, show the surprising similarities.
Traditionally, these individuals are young and socially retarded men initially becoming passionate of computer technology through role-playing games. Such entertainment, necessitating immoderate downloads has led hackers to manipulate telephone exchanges. The ordinary justification for their actions has included anti-establishment beliefs that inferred the corporate structures and government entities being designed to abridge individualism and discourage the collective unity. In addition, original hackers have emphasized the vitality of cyber-space arguing that Internet is a field of unreality, where nothing is real and everything is simulated.

7. What are anonymizers, and what is their relevance to the computer crime and investigations?

Anonymizer is an online service that transfers the trail of data that you leave while surfing. The anonymizers differ in their level of safety and quantity of features required. Some anonymizers demand the use of individual software; and another demand you log into their website before surfing other sites. However, anonymizers frequently used by individuals are determined to escape from the consequences of engaging into illegal, disruptive or socially wrong behavior online. Unfortunately, a big amount of child pornography downloaded through the web is entered through anonymizers. In addition, they are used to avoid Internet technologies that limit the online content entrance to certain amount of minutes or the amount of data.

8. What events precipitated the development of the enhanced data safety measures taken by the federal government?

Whilst during the Gulf War, the American security officials were forced to enhance safety measures. This happened after a laptop containing secrets of the allies’ war plans had been stolen from an official car while the Wing Commander it was assigned to was car shopping. Also, this lesson has been recently learned by the State Department after an inventory search initiated due to the theft of the laptop containing top-secret arms control data. This inventory has revealed that more than 15 additional laptops were not accounted. After this embarrassment and
public relations disaster, the State Department has reportedly tightened its security measures and established the firm parameters of accountability for laptop users.

9. What are the three categories of the computer crime? What are some of individual crimes included into each?

There are three categories of computer crime that serve as a basis. Firstly, it is spamming or sending mass emails. It is considered to be illegal. The cause spamming can be completely legal in some countries, as spammers are difficult to prosecute.

Computer fraud has different forms, including changing the computer input and result, changing or deleting the stored information, and changing or misusing system tools and software packages for some fake purposes. Any illegal data saved on a computer are also considered to be a computer crime.

10. How have the organized criminal syndicates utilized computer technologies to further their criminal interests? What are the implications for the future?

The computer data may also be utilized by criminal syndicates. Japan’s yakuza, experts at the practice of extortion, could significantly harm, if not destroy, the whole corporation by compromising the personal information residing within its computer system. Unfortunately, in future, crime syndicates will provide such activities more and more. And it is hard to control this activity all over the world.

11. What are some of the laws which have specifically targeted the online criminal behavior? Have they been applied effectively? Why or why not?

Fortunately, the federal and state legislators have developed a variety of laws to punish those ones responsible for computer contaminants. Creating and distributing a computer virus may constitute a variety of state-level offences including vandalism, trespass, harassment, the destruction of property and violation of a number of federal laws, including the computer fraud and abuse act, among many others. A New Jersey computer programmer that created the Melissavirus, for example, is currently facing charges of interception of public communications,
theft of computer services and conspiracy. He has received a penalty of 40 years and almost $500,000 of fines.

Chapter 5

1. *Name and briefly discuss the broad categories that phishing is split into.*

   Phishing emails divide into two wide categories: those which propose something that sounds too good to be true; or those which push you to update the security information threatening the account closure or suspension if you do not agree with them. These types manage you to fraudulent sites with the specific intention of getting you to supply with the personal information which they use for illegal purposes further. This can be done by either entering your accounts or pretending to be you in order to steal goods and services. Phishing attacks can also be sent by a message and text. However, they will still direct you to enter your data at a fake website which may look entirely genuine.

2. *A criminal activity facilitated by the identity theft/fraud is a four-phase process. Discuss and give the examples of each.*

   It has started with obtaining the identity through robbery, computer hacking, fraud, chicanery, power, redirecting or intercepting emails or even by some lawful means (e.g., purchasing the identification data on the Internet). At the second level, there is a possible use of identity for a fiscal gain (the most ordinary motivation) or keeping off the arrest or otherwise concealing the one's identity from the law enforcement or other authorities (such as invoice collectors). Crimes in this level may cover such as: account takeover, opening new accounts, a broad use of the victim's debit or credit card, selling the identity data in the street or a black market, obtaining the additional identity-associated documents, i.e. driver’s licenses, passports, visas and health insurance cards, among many others. Also, it could be filing fraudulent tax returns for big refunds, insurance fraud and robbery of rental cars. At the third stage of recognizing the theft is many misuses of credit cards that are discovered rapidly. The identity theft may take from six months to several years to find out. A proof suggests that the longer it
takes to discover the theft, the greater the deprivation incurred by a victim containing or not containing the law enforcement is. Considerably, more investigation is needed in this field.

3. *Bring out the contrast between the identity theft and identity fraud.*

Identity theft entails a process of illicitly obtaining someone’s personal information. Meanwhile, identity fraud entails using the data to commit a fraud. The use of fictitious identities to commit fraud also constitutes identity fraud.

4. *Briefly describe each of the physical methods of an identity theft.*

Physical methods provides stealing your mail searching through the trash you throw out, hoping to find the important documents; stealing the information from your card; and the ordinary theft of your wallet or purse.

5. *Identity theft and fraud attract many different kinds of crimes. Discuss the crimes that are included into the text and list as many as you can think of.*

The most harmful is ID theft that occurs in the form of a Stolen Social Security Number. Cleaning up the disorder that occurs with credit card robbery is simply compared to the restoration and rebuilding needed after the oversized demolition that can take place from the public security sameness robbery.

Of the most menacing types of sameness robbery, a passport fraud could well verify to be a cause for warning. While the credit card sameness robbery and bank fraud threaten individuals and upset their individual accounts, the passport fraud at its most frightening level has the capacity to intimidate the security and safety of the whole nation.

6. *The text describes the difficulty in estimating the cost of victimization of the identity theft/fraud; explore these causes and discuss the lack of reporting issues in depth.*

Identity theft and the related fraud increased considerably in 2012 with 11.2 million victims for the estimated cost of $54 billion dollars. In 2008, just fewer than 10 million people were ripped off as a result of identity theft for an estimated cost of $48 billion. It is interesting
that the cost to individuals as a result of data breaches has declined from $498 in 2008 to only $373 in 2009.

Unfortunately, some of hidden costs exist. They even cannot be measured properly. Not surprisingly, victims have found that most of nervous reactions to being a victim of cybercrime are equivalent to those known by other crimes’ victims, i.e. burglary. Victims have reported feeling mad, cheated, and annoyed. They did not believe that their attackers could be caught or punished. Thus, experiencing a cybercrime is almost identical to being vandalized or burglarized. When an unauthorized person else enters/uses your space, whether it is your house or your computer, takes and damages your assets, then you ought to feel violated.

Chapter 6

1. List and describe the methods of online communication among terrorists.

The jihads terrorists use web for communication. They share a single email account and the individual writing that the message is not sent further but saved as a draft. Then, a recipient logs into it and reads the draft without ever actually being transmitted. In addition, the jihads have communicated on gaming forums and even once on a bike forum. Rarely, they use a "live chat" functioning on Japanese gaming sites. Jihad web sites change their URL every time. They are password-protected from Western countries’ viewers. They are also language-protected as the communication is in Arabic. Jihads simply write URL in the Arabic language, so the U.S. computers or non-native speakers do not understand it.

2. Explain different classifications of motivation of terrorists.

The first classification of terroristic motivations is separatist groups’ motivations. They reach for an aim of dissociation from the existing entities through liberty, governmental independence or authority. The ideology that separatists maintain covers the collective fairness or equity, anti-imperialism as well as the opposition to conquest or control by an extrinsic power. The categories of such ethnicity and nationalism can crossover in the support rationale.
Ethnocentric groups review race as a main attribute of people and an essence of cohesion. Group members support the position that the particular group is preferred because of its ethnic or national characteristics.

The faithfulness and allegiance to the country and national consciousness point the nation’s background and interests above those of other nations or groups is a motivating element behind nationalistic criminal groups. This can be an aim to make a new nation or to split away some of existing states in order to unite with another nation that shares the perceived national sameness.

Revolutionary groups are dedicated to the overthrow of the established organization and replacing the governance with a new political or collective order. Often associated with communistic political ideologies, other political movements can advocate for rebellious methods to accomplish their goals.

3. Discuss Osama bin Laden's role in incorporating Internet in his terrorist group.

Osama bin Laden has combined multimedia propaganda and advanced the communication technology to create a very intelligent form of psychological influence. He and his followers have moved their propaganda efforts to the Internet, where visitors to al Qaeda’s numerous websites and to the sites of connected organizations can access prerecorded videotapes and audiotapes, CD-ROMs, DVDs, photographs and announcements. Unfortunately, Osama bin Laden has left inheritance for other terrorists and showed how they can use Internet for their interests.

4. How are terrorist groups and organized crime groups similar in their modality and criminal operations?

If we look at the similarities among the organization and the evolution of terrorist groups and organized crime groups, we can see some existing interconnections. There are such interfaces between terrorism groups and organized crimes:

1) Terrorists get engaged in an organized crime to make money.
2) Terrorists and organized crime groups often work within network structures, and the structures at times intersect; terrorists may hide among the criminal organizations that are transnational.

3) Both groups operate in areas that are not strictly controlled by the government and have weak laws and regulations.

4) Either organized criminals or terrorists wick their regional powers to accomplish their goals.

5) Terrorists and organized crime groups often use almost the same means of exploitation of the latest technology.

6) Both groups use the same methods and at times even the same operators to control and move their cash funds.

5. How has technology changed the face of the organized crime?

The fast evolution of Internet increasingly develops the international trade and, in turn, provides some possibilities for the organized crime. A huge number of online users as well as the fast speed, in which the financial transactions occur, require the law enforcement to remain in step with some current technological devices and equipment.

As the technologies for conducting online commercial transactions have evolved, so opportunities for fraud do. Identity theft and payment card fraud are the most frequently used types of fraud. Identity theft provides some opportunities for criminals to provide a false identity and obtain funds illegally. The use of sophisticated peripherals such as laser printers, digital cameras, scanners and desktop publishing software can help to provide the production of false identities and counterfeit documents. Email is alternatively used to provide schemes such as the stock market manipulation, frequently named as “pump and dump or slump and dump” schemes. Criminals such as outlaw motorcycle gangs and Asian criminals are using the technologies to secure their documents and communications.

6. List the contemporary characteristics of organized crime groups.
The contemporary groups of organized crime, whether usual mob families or row gangs, are distinguished by a number of general characteristics, such as:

1. An organized crime prospers on illegal supplying of certain services and goods for which many people are more than willing to pay.

2. The aim of organized criminal groups is to create money. Participants also get a reason of self-respect, power, and defense.

3. Groups have got what is named a pyramid of the major power complex body part. In lawful businesses, there are bosses, vice presidents, executive officers, advisors, accountants, treasurers, lawyers, and other specialized staff. Organized criminals have a chief; advisors that are closely operating with their boss and delegate tasks to various crews; captains running several crews; soldiers conducting a physical function and acting tasks from accumulating of money to murdering of people; and the manpower with specialized skills.

4. Members are highly hard-core and pledged. They take oaths and pass institution rituals.

5. Penalties for the members that stray include demotions to lower ranks.

Chapter 7

1. What actions has the federal government taken to legislate online behavior? How have these mandates evolved over some time?

In 1998, the first main legislation made its way through the Congress and was passed into law. The Children’s Online Privacy Protection Act (COPPA) of 1998 was the first law of such type. The law protects the secrecy of minors by legislating that online entities will not procure the child’s individual data without a parental permission. It also outlaws requiring minors to provide more data than are necessary to play a game online or participate in a competition. All websites must also create their privacy policies available to parents. Also, the federal and state legislators have developed a range of laws to penalize those authoritative for computer contaminants. Creating and distributing a computer virus may constitute a diversity of national-level offenses including vandalism, trespass, harassment, demolition of property and
infringement of a number of federal laws, including the computer fraud and abuse act. A New Jersey computer programmer that has created the Melissavirus, for example, is currently facing some charges of interception of community communications, robbery of computer services and connivance. He could get a punishment of 40 years and almost $500,000 in fines.

2. How may the traditional statutes be applied to the contemporary phenomenon of computer crime?

Legislation at the federal and national level applies for the prosecution of the computer crime. In addition, computer crimes could cause some proceedings using federal laws. They are exclusively concentrated on the computer violation. Many proceedings do not utilize these special computer-associated statutes. Thus, prosecutors often go on to use the usual criminal laws in computer crime prosecutions. Although computer crime statutes improve to adapt to the new forms of illegal actions, the law has moved slowly in contrasting to the fast evolution of computer technology.

At the forefront of some federal computer-associated offenses, there is a computer deception statute of 1984 (The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984). This computer crime statute prohibits 7 different types of computer-associated actions. They are such as: (1) electronic spying; (2) illegal access to the fiscal formation data, the data from the US department or agency, or the data from any secured device concerned in between the state or outlandish business; (3) globally surfing in a Ministry computers or affecting an administration computer; (4) using the computer for the schemes of deception or robbery; (5) transferring software that causes harm or entering a protecting computer and causing injury; (6) between the state trafficking of passwords; and (7) blackmailing threats to a protected computer.

One more federal statute that provides the prosecution of computer-associated actions is the Economic Espionage Act of 1996. This act has concentrated on the defense of trade secrets. Trade secrets, a word formulated in the statute, cover an array of different types of data that have a real or future value and that a holder has "taken rational measures" to keep encrypted. The
Economic Espionage Act proposes a trade secret saving to businesses and the state government. The point of data to the public and the cases that are joined to protecting these data, establish the EEA as a significant move in how the law can accommodate the protection from the computer violation.

4. Briefly, describe the recent additions in Europe's CoE.

A survey of the Council of Europe strategies on cybercrime shows the progress in the fields of political support and extended partnerships in the Budapest Convention, the effectiveness of this treaty through some equal assessments, the adoption of the report on a trans-border access to information and the capacity building.

In 2013, more States will join such Budapest Convention. Also, there will be some providing steps towards a more effective global cooperation, the launch of a new common project of the Council of Europe and the EU to support the countries all over the world in the implementation of the Budapest Convention.

5. Discuss and describe the most recent statute in relation to identity theft showing why it is significant and how it aids the cause to slow identity theft.

The Identity Theft and Assumption Deterrence Act of 1998 is the first piece of the federal legislation to deal with identity theft. The follower Act to the Identity Theft Penalty Enhancement has established the fees for identity theft. It contains some instances when identity theft has been used as one piece in the process of more serious crimes, such as terrorist acts, immigration violations and firearms offenses. The Part five of the Fair and Accurate Credit Transactions Act, an amendment to the Fair Credit Reporting Act, refers to identity theft and the related cases. Victims of identity theft are given the ability to work with creditors and credit bureaus to move the negative data in their credit reports resulting from identity theft.

6. How is the partnership of professional associations useful?

The Identity Theft Protection Association is a global organization for professionals, service providers, businesses, law enforcement and other sides being evolved in and upholding
the joint aim of reducing identity theft, privacy and information safety risks. The ITPA and its
worldwide network of members teach, communicate and regulate to solve identity theft, privacy
and data security risks. This association has set some new standards and protection to
participants and the public. The ITPA offers some unique and professional resources as well as
broad opportunities for the recognition, training and teaching. Membership is available for
professionals and organizations all over the world.