**Security and Fraud Study Questions**

1. **Define fraud.**

Fraud is any means a person uses to gain an unfair advantage over another. Fraud usually involves the misrepresentation of facts about a situation and the reliance on that misrepresentation by the victim. Frauds are often called "cons" because they involve a violation of trust or confidence.

1. **What are the two kinds of fraud in business?**

Employee Fraud is a misappropriation of assets, or theft, by a person or group for personal financial gain. Fraudulent financial reporting is intentional or reckless conduct that results in materially misleading financial statements.

1. **What are the actions recommended to reduce the possibility of fraudulent financial reporting?**

Establish an organizational environment that contributes to the integrity of the financial reporting process. Identify and understand the factors that lead to fraudulent financial reporting. Assess the risk of fraudulent financial reporting within the company. Design and implement controls to provide reasonable assurance that the fraudulent financial reporting is prevented

1. **What are the three common things that happen in a fraud?**

Theft of an asset. Conversion to cash (if not already cash). Concealment of the crime

1. **What is a computer fraud?**

Computer fraud is any illegal act for which knowledge of computer technology is essential for its perpetration, investigation, or prosecution

1. **Why is computer fraud on the rise?**

Not everyone agrees on what constitutes computer fraud and some people may commit computer fraud unwittingly and not be aware of it. Many computer frauds go undetected. The belief that "it just can't happen to us". Most networks have a low level of security. Many Internet sites provide guidance on how to commit computer crimes. Law enforcement is unable to keep up with the number of computer frauds.

Most frauds are not reported. The total dollar value of losses is difficult to calculate.

1. **How can a system be protected from viruses?**

Install reliable antivirus software that scans for, identifies, and isolates or destroys viruses. Use caution when copying files on to your diskettes from unknown machines. Ensure the latest versions of the antivirus program available is used. Scan all incoming emails for viruses at the server level. All software should be certified as virus-free before loading it into the system. If you use jump drives, diskettes, or CDs, do not put them in unfamiliar machines as they may become infected. Obtain software and diskettes only from known and trusted sources. Use caution when using or purchasing software or diskettes from unknown sources. Deal with trusted software retailers. Ask whether the software you are purchasing comes with electronic techniques that makes tampering evident. Check new software on an isolated machine with virus detection software before installing on the system. Cold boot to clear and reset the system. When necessary, "cold boot" the machine from a write-protected diskette. Have two backups of all files. Restrict the use of public bulletin boards.

1. **Discuss antivirus software programs.**

There are three types of antivirus software programs. Virus protection programs are designed to remain in computer memory and search for viruses trying to infiltrate the system. When an infection attempt is detected, the software freezes the system and flashes a message to the user. Virus detection programs spot an infection soon after it starts. Virus identification programs scan all executable programs to find and remove all known viruses from the system.

1. **How does a company make fraud less likely to occur?**

A company can decrease fraud by: good hiring and firing practices; good management of unhappy employees; training in fraud awareness; manage and track computer licenses; implement signed confidentiality agreements; maintain visible security; educate the workforce in ethics and the penalties for illegal acts.

1. **How can companies reduce losses from fraud?**

Maintain adequate insurance. Keep a current backup copy of all program and data files in a secure off-site location. Develop a contingency plan for fraud occurrences and other disasters that might occur. Use special software designed to monitor system activity and help companies recover from frauds and malicious actions.

1. **What are some of the distinguishing characteristics of fraud perpetrators?**

In the case of computer criminals, they are often young and have substantial computer knowledge. About two-thirds are men and likely to be an employee of the firm from which they steal. Many are unhappy or disgruntled with their employer because they feel unappreciated and underpaid. Most have no previous criminal record.

1. **What is the difference between a worm and a virus?**

A computer virus is a segment of executable code that attaches itself to computer software. A virus has two phases: it replicates itself and spreads to other systems or files, and in the attack phase, the virus carries out its mission to destroy files or the system itself. A worm is similar to a virus, except that it is a program rather than a code segment hidden in a host program. A worm can reside in e-mail attachments, which when opened or activated can damage a user's system. Worms can also reproduce themselves by mailing themselves to the addresses found in the recipient's mailing list. Worms do not have long lives, but their lives can be very destructive nonetheless.

1. **What are some of the computer fraud techniques used by perpetrators?**

Various computer fraud techniques include: Trojan horse - unauthorized code hidden in a legitimate program. Round-down technique - rounded off amounts from calculations and the fraction deposited in perpetrator's account. Salami technique - small amounts sliced off and stolen from many projects over a period of time. Trap door - bypass of normal system controls. Superzapping - use of a special program to bypass regular controls. Software piracy - unauthorized copying of software, probably the most committed computer crime. Data diddling - changing data in an unauthorized way. Data leakage - unauthorized copying of data files. Piggybacking - latching onto a legitimate user in data communications. Masquerading or Impersonation - the perpetrator gains access to the system by pretending to be an authorized user. Social engineering - a perpetrator tricks an employee into giving him the information he needs to get into the system. Logic bomb - idle until some event or time triggers it. Hacking - unauthorized access and use of a computer system. Scavenging - gaining access to confidential data by searching corporate records in dumpsters or computer storage. Eavesdropping - observation of private communications by wiretapping or other surveillance techniques. E-mail threats - threatening legal action and asking for money via e-mail. E-mail forgery - removing message headers, using such anonymous e-mail for criminal activity. Denial of service attack - sending hundreds of e-mail messages from false addresses until the attacked server shuts down. Internet terrorism - crackers using the Internet to disrupt electronic commerce and communication lines. Internet misinformation - using the Internet to spread false or misleading information. War dialing - searching for idle modem by dialing thousands of telephones and intruding systems through idle modems. Spamming - e-mailing the same message to everyone on one or more Usenet groups.

1. **Why do fraudulent acts often go unreported and are therefore not prosecuted?**

Most fraud cases go unreported and are not prosecuted for several reasons. Many cases of computer fraud are as yet still undetected. As new technology and methods become available to organizations, prior undetected fraud may be revealed in the future. A second reason is that companies are reluctant to report computer fraud and illegal acts simply because of bad publicity--a highly visible case can undermine consumer confidence in an organization such as a financial institution. Also, the fact that a fraud has occurred may indeed encourage others to attempt to commit further acts against the organization. It would seem that unreported fraud creates a false sense of security, as people think systems are more secure than they are in reality. Another reason for not reporting fraudulent acts is the fact that the court system and law enforcement is busy with violent crimes and criminals in its system. There is little time left to go after a crime where no physical harm is present. Also, the court system tends to treat teen hacking and cracking as "acts of childhood" rather than as serious crimes--this leads to many plea bargains when a computer fraud is brought to trial. Another reason is that a computer fraud case is difficult, costly, and time-consuming to investigate and prosecute. Before 1986 no federal law existed governing computer fraud. Law enforcement officials, lawyers, and judges generally lack the computer skills necessary to properly evaluate, investigate, and prosecute computer crimes. Sadly, when all is said and done a successful prosecution and conviction of computer fraud results in a very light sentence. All of these factors contribute to the underreporting and lack of prosecution of computer fraud crimes. Not everyone agrees on what constitutes computer fraud:

* Many networks have a low level of security
* Many Internet pages give instruction on how to carry out computer crimes
* Law enforcement has difficulty keep up with the growing number of computer frauds
* The total dollar value of losses from computer fraud is difficult to estimate.