# Computer Crime

Unit

11

# Unit 11

# Computer Crime

**Learning outcomes**

**By the end of this unit the learner will be able to:**

- **Understand what is Computer Crime**
- **Explore the Features of the Computer Environment**
- **Identify the Types of Computer Crimes and Source of Digital Data**

## Introduction

Modern technology plays several different roles in the fraud environment. In order to prevent, identify and investigate fraud, computer systems and data can be used. Whenever technology is used by individuals to commit fraud, a computer is the mechanism used most frequently. A computer is defined broadly here, as a device which performs calculations and stores data. Servers and computers are technologies that can even be the target of criminal activities including financial fraud.

White and blue collar crimes have been in existence long before the presence of computers; however, there were no computer crimes then. In those days, crimes were committed against people and property. The evolution of computers did not invite a new crime wave; it simply changed the form of previous crimes. Generally, crimes related to computers are occupational crimes, which means that they are committed mostly by insiders or previous insiders who possess the requisite knowledge, skills, and access. This is because unauthorized access can be gained more conveniently by organization insiders or employees than by outsiders. Studies on crime have found approximately 70% to 80% of crimes to be malicious computer-related acts.

The most effective evidence in almost any individual fraud case could be gained from several various sources. The best evidence could be obtained from an interview, digital information or paper documents. Digital information has become more common in frauds and includes information in e-mails, digital files the fraudster erased, notes made in computer files, and several other sources, especially information of a personal nature. Increased possibilities of finding forensic evidence in computers is due to the exponential growth in the presence of technology in our community.

## Computer Crime Theories and Categorizations

Computer system crime can be viewed as either a crime against computers or through using computers to commit a conventional fraud or crime, such as fraudulent financial statements, fraudulent disbursements, etc. It is a fact that fraud principles, specifically the fraud triangle and the fraud tree apply to computer crimes as well, as they do to other

crimes. A theory of computer-related crime is a concept referred to as MOMM, which is similar to the fraud triangle but specific to computer crime.

### Computer Crime Theory: MOMM

MOMM is a short form for motivations, opportunities, means, and methods. It can be observed that the first two terms come from the fraud triangle, leaving only the rationalization leg. Financial motives signify that people who commit frauds have money as a main objective. They reflect the need to secure a financial advantage from the crime. The object of the fraud may not be only money, it could also be something that can be converted into or exchanged for money.

Ideological intentions are displayed when the perpetrators feel motivated to seek revenge against someone or when they believe something is exploiting or oppressing them, not necessarily involving any financial motive. Acts of stealing classified information for foreign entities is often conducted for ideological or political reasons. Damage to computers by unhappy employees is another example. Such criminals may think that computer technology is a threat to their economic and political survival or well-being, or may simply be seeking revenge.

Egoistical motives are those associated with power, egos, and pride. Most frauds include this motive to some extent. Young enthusiasts who seek the thrill of the challenge to commit computer frauds or crimes exhibit egotistic motives. Psychotic motivations include an exaggerated fear of computers, a distorted sense of reality, misconceptions of persecution or of grandeur. There have been fewer reported incidents where psychotic motives were the reasons for computer abuse.

Environmental conditions that have provided motivations for computer related crime and abuse include both the external environment, such as the world or marketplace and the internal environment of the firm that operates a computer. Internal effects that can add to the motivation for computer connected crime and exploitation include:

- Work environment
- Level of interpersonal trust
- Reward system
- Level of ethics in the entity's culture
- Level of effectiveness of internal controls
- Level of stress, such as the pressure for performance
- From the outside, motivations for computer linked crime and manipulation may be provided by the current ethical and social values of society, economic conditions in the country or the world, and competitive conditions in the industry.

### Computer Crime Categorizations

Computer crimes could be categorized by the loss to data, such as availability, confidentiality, integrity; or the type of crime, such as theft and fraud; or the type of loss caused, such as financial or physical damage. The computer could be the target of the criminals where the objective of the crime is destroying computers, denial of service, etc. The computer could be the instrument used to commit the crime, for example, online identification theft, fraudulent second set of accounting data, etc.; or incidental in another crime objective.

Computer crimes can also be grouped into three simple categories that are comparable to the three stages of data processing: namely, input, process or output.

- Input crimes involve the entry of false or fraudulent data into a computer; data has been altered, counterfeited, or forged, lowered, raised, destroyed, intentionally omitted, or created.
- Processing crimes include the altering of computer processing for fraudulent means for example; attacks such as denial of service that alter systems processing to affect losses to the victim or the ill-reputed schemes exposed in Superman and Office Space where programmes round interest calculations and route the remaining amounts to personal accounts.
- Output crimes, such as theft of computer-generated reports and data files seems to be increasing in this era of intense competition, for example customer mailing lists, research and development results, secret formulas, long-range plans, employee lists, etc.

Another categorization of fraud crimes is internal and external. Internal crimes are much greater in number. The most common type of computer crime is, in fact, a theft of assets by employees. They have fraud opportunity from being inside the organization; the fraud triangle is complete with some pressure to steal, such as personal cash flow problems and weak personal ethics. The temptation can become too great for the employee to resist stealing from the organization if a weakness is present in the controls. Then there are those who break in from the outside to steal data, spy or sabotage systems. Others bring a system down and make it unavailable to users.

## Characteristics of the Computer Environment

Manual accounting systems have progressed naturally into computerized accounting systems. However, they still possess special characteristics that make them more vulnerable to crime. It is necessary to understand these features in order to understand the potential influence and extent of computer-related crime.

### Connectivity

The ability to transfer messages between independent devices is called computer communication. The computer devices must be connected in some way in order to communicate. Susceptibility to computer crime is increased with the increase in connectivity of information technologies, because the connectivity that facilitates the desired benefits also facilitates undesired crimes.

The Internet aggravates risk as it opens the network up to anyone in the world with the knowledge and opportunity to commit computer fraud. Any computer expert can be motivated to attack an organization's computer. The basic value of the Internet is that it provides the opportunity to connect from virtually anywhere, almost at any time to millions of computers around the world. The disadvantage of the Internet is the increased complexity in systems, attacks and the ability to recognize who did what, how and when.

The idea of connecting computers continues to develop and takes on new forms. Networks are now connected wirelessly, with numerous types of other networks and ''clients'' (devices to connect to a network such as a BlackBerry or Personal Digital Assistant), through a virtual private network (VPN).

Computer systems become more vulnerable as they are open to the Internet or external systems. Information can be stolen by tapping into communication mechanisms or by copying it through a workplace. There can be illegal entry through Internet access or public telephone lines. Data can be downloaded remotely to a nearly invisible flash drive. In the event that an undesirable event takes place, computer based crimes can have tremendous impacts due to their viral nature.

### Concentration of Data

Data that is stored in computers is increasingly considered to be an asset capable of causing the transfer of money. Data transfers allow financial transactions to occur in a variety of ways, at any time, quickly, and remotely. But data also has value in another sense because of its concentration. Although data is not a negotiable instrument (as is a bank check), however, it has intrinsic value. Digitized objects make up scientific data files, confidential programmes, confidential financial information and programmes that a company can sell for a profit.

Computer systems combine and collect data from all departments within an organization. This data is processed and typically stored centrally. The presence of data in one location makes this data vulnerable to other risks, but centralization for security purposes can be beneficial for certain risks. In some cases, a person can access any or all of a company's financial data or other digital records simply by obtaining the appropriate password, excessive unauthorized access, or ability to override controls. Data also suffers from physical damage due to system failures or human error, which can destroy records forever if a contingency plan does not exist or does not work.

### Positions of Trust

Due to the nature of their jobs, programmers, database administrators, and data entry clerks are in a position to manipulate the records. A high degree of trust must be placed in the people in these positions, but the positions and people present a high degree of risk. Generally speaking, for a fraud to occur, the person had to be trusted first.

Several computer analysts and programmers are not well-informed about the general principles of internal control or accounting controls. Thus most systems are designed without adequate controls. Frequently they are standardized, not customized to the organization's structure and processes. Many programmes that have been operating for a long time have undergone extensive changes that are poorly documented. The ''patched'' programmes can be hard to understand, and it is possible that only a few workers are able to support them. If the systems are still maturing, they will have extensive programme changes, data conversions, and other projects occurring if systems are current. Either way, anyone with sufficient knowledge of the given computer area could possibly manipulate or change programmes or data to their benefit without the change being discovered.

Other important features of the computer environment include:

- Complicated technology: Understanding the integration and substance of technology is challenging and requires knowledge and an ability to see through the technical aspect of systems.
- Unclear audit track: Large volume of transactions, together with the networks and online access available on many systems may result in an incomplete or confused audit trail.
- Direct access: Access to systems is continuously available, abundant and challenging to maintain.
- In-built insecurity: The hardware and software used today was designed without much real security, and even secure technology must be updated continuously.

## Types of Computer Crimes

There are many forms of computer crimes, including intellectual property theft or violations, child pornography, software piracy, online gambling, spying and hate crimes. The following list represents only some types of crimes because covering all types of computer crimes is not feasible.

### Identity Theft

Thieves steal physical items such as credit cards or their data, or they steal login identifications for financial accounts, or even someone's identity. There are various ways a criminal might steal someone's identity, including data theft through social engineering or excessive access, or sniffing (software programs that capture Internet messaging) or spyware. The issue of identity theft continues to grow and will continue to grow in the foreseeable future.

### Blackmail

Internet blackmail is an area of high criminal activity, with targets such as online casinos, technology and security companies, and who knows what others, because victims generally do not report blackmail publicly. Swindlers, mafia, and street gangs have increasingly switched to computer-based operations, and often use blackmail or other threats. Ransoms from these attacks have been reported in millions of dollars. People must immediately seek the help of a technology specialist and a lawyer if they encounter this type of crime.

### Denial of Service Attack

A DoS attack is carried out to harm victims in a different way. Different forms of Denial of Service attacks exist, and include DDoS and reflection DoS attacks. All of these malicious objects attempt to bring computer systems down, particularly online web servers that provide e-commerce. When firms such as eBay, Amazon, and Yahoo! are down, not only do these entities have no means of conducting business operations during that time, but criminals also gain publicity from their acts because they are high-profile businesses.

### E-Mail Attacks

Criminals use different forms of despicable e-mail attacks, including viruses, spamming, spoofing, and spyware. Spam is unwelcome e-mail or junk e-mail. Spamming techniques can be used to block an e-mail server to the point that it locks up. The Christmas Virus was one of the first so-called viruses released into IBM's computers. A Christmas card message was sent that contained programming code to replicate the message to everyone in the recipient's address book, locking up IBM's systems for quite some time. Spamming the right system with the right code can work much like a DoS attack.

### Cyber Forensic

This involves the effective capture, preservation, identification, extraction, analysis, and documentation of digital data and events. One way of viewing the cyber forensic process is like any other type of forensic investigation, where the professional is looking for forensic evidence that will stand up in a court, and will provide something similar to a fingerprint that helps to identify the culprit.

### Expectation of Privacy

One important element of obtaining cyber evidence, or any other fraud evidence, is the legal policy known as expectation of privacy. This policy is actually associated with and comes from the Fourth Amendment:

"The right of the individuals to be safe in their persons, papers, houses, and effects against unreasoning searches and attacks, shall not be violated, and no warrants shall issue, but upon doubtless cause, supported by oath and confirmation, and mainly describing the place to be searched, and the things or persons to be held."

This relates to those who commit fraud against the entity, and the expectation of privacy relates to that person's office space and all of the things in it. As it is also related to cyber forensics, that would extend to the employee's computer, USB drives, corporate cell phone (or similar device), CDs, external drives, DVDs, and any other source of digital evidence. A sudden search or capture of that person's possessions, including the company's technologies could be a violation of that person's expectation if the employee has reason to expect that his or her privacy is respected in the workplace, or put another way, a violation of that person's rights under the Fourth Amendment. Therefore, it is important to first make sure there will be no violation of privacy if any fraud investigation includes the need to obtain sources of potential evidence, especially digital in nature, from an employee's office.

### Types of Investigations

For a cyber-forensics investigation to take place, there has to be an event that initiates it. The initiation event and decisions are critical to the success of the subsequent cyber investigation. Basically, the investigation will be one of these two types: a public investigation or a private investigation. Both of these are very different and each has its own limitations and needs in the cyber forensic case.

### Public Investigations

Public investigations include a potential violation of a law creating a potential criminal prosecution. The investigation needs to be conducted in a way that will comply with legal requirements and procedures, because the potential criminal trial includes a law and the accompanying criminal court procedures. For instance, cyber forensic evidence will need to address the violation of the law and the legal requirement to prove the criminal offense. The victim needs to consider the publicity impact of the event since the event will become public. The investigator will need to understand the restrictions of custody of evidence, expectation of privacy, and other critical concerns in a public investigation.

Custody of evidence includes knowledge of proper legal protocol for acceptable forensic or other evidence in the courtroom. Those rules of evidence affect the hearing of the case in court and the original capture of the cyber evidence, and are called a proper chain of custody. Thus the cyber forensic specialist (CFS) understands what can or cannot be done at the crime scene, and what steps or precautions must be taken to preserve the potential evidence, when sources of potential cyber forensic evidence are captured.

The CFS understands the types of actions or things that will alter or damage the potential evidence according to the legal perspective. For example, if anyone, including a representative of the victim organization, accesses the suspect's computer (assuming it is a Windows system) and browses around looking for evidence, that act will provide defence counsel with grounds to dismiss the evidence. The defence may show the dates accessed in Windows Explorer and make the claim that the last person to access the computer is the one who put the incriminating evidence on the computer.

Secondly, due to the consideration of expectation of privacy, an important element here is the need for a search warrant, particularly for a public investigation. A search warrant will have to be obtained before the CFS begins to capture evidence, because it is a violation of a criminal law, and because of the Fourth Amendment rights. Skipping this step could cause the potential evidence to be banned in court and lead to a violation of Fourth Amendment rights of the suspect.

### Private Investigations

The cyber forensics investigator should understand the limitations and investigative requirements of evidence, subsequent trial, expectation of privacy, and other issues in a private investigation, which are different from those in a public investigation. For instance, a private investigation is not ruled directly by Fourth Amendment rights. However, the investigation should consider expectation of privacy in a fraud investigation as a safety measure.

The private type frequently involves a dispute or potential violation of the entity's policies and procedures, or a crime such as fraud. In the case of the former, issues might include unacceptable e-mail activity, discrimination and alteration of corporate data, etc.

Private investigations can become public, because of circumstances or evidence that develop during an investigation. During or after the fraud investigation process, the victim may decide to pursue civil litigation or criminal prosecution. In these cases, the attorney or prosecutor will often not understand cyber and digital evidence sufficiently well to present it in court without assistance from an expert. The CFS can provide value to the private investigation by educating and assisting lawyers or prosecutors in providing an explanation of the digital evidence but by collecting effective cyber evidence to support the case.

## Sources of Digital Data

Rich digital sources of evidence and information are available in a cyber-forensic investigation. Cyber forensic specialists have familiarity with the different available and applicable storage devices. Fraudsters can hide data in many ways by moving it from organizational systems to their own computer or by placing it on a removable, portable device; or using unknown storage devices from the start. Such devices include:

- Home computer
- Office computer
- Network servers
- Laptop
- Backups
- Internet service provider (ISP) servers
- Flash drives (USB/thumb drives) can be concealed as a normal fountain pen
- Removable external drives
- CDs

- Digital watches
- DVDs
- Memory chips of digital cameras that can be concealed under a postage stamp or a digital camera in plain sight due to their very small sizes
- E-mail accounts: business and private
- Printer memory
- Voice mail
- Cell phones (including Blackberry, iPhone, Droid, and other smartphones)
- Personal digital assistants (PDAs)

Care should be taken to differentiate personal sources of digital data from organizational ownership. Such as, if an employee uses his or her own cell phone and links it to a corporate Outlook system, who owns the data on that cell phone? Can employees secretly take valuable organizational information with them on that cell phone? The same is true about the need for a search warrant, if the victim suspects that the perpetrator stored evidence on personal computers or storage devices not located on the buildings of the organization.

## Types of Cyber Data

Fundamentally, cyber digital data takes on three forms: extractable digital data, metadata and latent digital data.

### Extractable Digital Data

This data may be defined as observable, not with the naked eye but with the right technology. For example, digital data stored from an Excel spread sheet on a hard drive is extractable, but hardly visible to the eye. However, it clearly becomes visible to the eye, if one uses the right version of Excel, and can locate and access the digital file. Extractable data then is subject to familiarity with the right tools and techniques to locate and convert it to observable data and information.

Extractable data also includes data files that can be ‘‘mined’’ for all intents and purposes to uncover irregularities that are hidden in the quagmire of data. Data withdrawal tools can be used on accounting data files to look for proof of a fraud. A digital investigator (or fraud auditor) has the possibility of uncovering any type of fraud, by combining awareness about fraud schemes with knowledge of the red flags of fraud schemes.

### Metadata

Metadata can be defined as data about data, such as a formula behind a cell in Excel is metadata, describing how the data being displayed was developed. Metadata is normally stored by applications or developers and is a potential source of valuable information or evidence. All Microsoft Office products have properties metadata that contains a treasure of user-defined metadata about the file, and also include data added as defaults. It also includes the dates associated with the file (created, last modified, and last accessed), file location, file name, and certain stats. Metadata can be an isolated file external to the object

file or can be embedded internally to the digital file. Either way, the default information in metadata can be helpful in extracting useful evidence. Some of the types of metadata include:

- Spread sheet data sources and formulas
- E-mail captions and routing information
- Database structure and relationships
- Word processing editing history (e.g., track changes, deletions/undo)
- Microsoft Office properties
- Windows NTFS/FAT library files (directories of files, sectors, and hard drive facts)
- Certain aspects of XML files
- System logs of users' activities
- Certain HTML code

### Latent Digital Data

This data is described as concealed, undiscovered, missing, misplaced or hidden data. Latent data is not easily converted to observable information by some common application or subject to data mining tools, under normal operating circumstances, and is generally transparent to operating systems and file managers. It takes special cyber tools, knowledge, and techniques to find and extract this type of cyber data.

Latent data includes digital data on hard drives that is not visible by the operating system or accessible by applications but was handled by the operating system. For example, when a user deletes a file using the operating system's delete command, the file is not actually deleted, but rather marked as available for future use by the library function (e.g. NTFS/FAT). For years, cyber forensics have had an ''undelete'' tool available to locate deleted files, and unless the space was used to record data subsequent to the delete, that digital data is fully recoverable.

Latent data is easily modified or destroyed because of its nature. Additional precautions are necessary to prevent any alteration to it. Latent data requires special tools and equipment. It requires one or more SMEs (specialized subject matter experts) who have the necessary training and experience in order to extract any potential evidence.

Examples of this type of latent data include:

- Deleted files
- RAM data
- Slack space (temporary files for downloaded files or images)
- Inter-partition space
- Windows swap files
- Temporary files
- Unused space (may still contain traces of previously existing files)
- Stored printer images

Another kind of latent digital data is the covert and deliberate embedding of data in unexpected places by a cyber-savvy criminal. There are several ways of placing digital data on storage drives in a sophisticated way that makes it difficult even for a CFS to locate and recover it. Essentially, the criminal hides application data on storage media or TCP/IP packets in places where the standards suggest it does not belong. Stenography is one way to accomplish this secret method of hiding data, which means the data is hidden in plain view of data that is recognized by applications, retrievable in some manner (extractable data) or observed by the operating system.

Latent data will become increasingly difficult to find as cyber criminals become more sophisticated. Latent data can be a source of potential evidence in a fraud investigation. A CFS is needed to locate and extract most of this type of data. Investigators should be skilled in data discovery planning to consider all potential latent data sources, because most of the latent data will very likely not be relevant to a case.

### Cyber Forensics Investigation Process

For a successful investigation, the cyber forensic investigation process is critical. The process is initiated when the investigation starts by a tip or other event. The victim, who has asked a CFS to be involved, will ask that person to evaluate the situation for potential evidence. It is the job of the cyber forensic expert to accurately identify all potential sources of evidence and information that could potentially be valuable to the investigation.

Although the next step is not the responsibility of the CFS, the team needs to resolve the expectation of privacy. If it is decided that a search warrant is necessary, the CFS will need to assist in developing search items to list on the warrant and to review the actual warrant for precision once it has been created.

Typical Cyber Forensic Investigation Practice

- Recognize all important digital sources of potential evidence of sources of information.
- Decide/consider expectation of privacy issue (search warrant details, if necessary).
- Acquire and validate digital/cyber evidence (without alterations).
- Protect original evidence (bag, device, establish chain of custody).
- Move evidence to secure forensics lab.
- Create copies of original device (without alterations to original).
- Confirm the copies of original device
- Develop precise cyber forensics tests, procedures, and overall plan (use formal procedures).
- Complete and file a report on evidence, analysis, and assumptions.
- Perform the plan using applicable forensic tools.
- Convert digital data into presentable form (e.g., graphs).

Subsequently the CFS will actually go with the main investigator or team to the crime scene and acquire the devices or equipment that contains the sources identified in the first step. It is critical that the CFS authenticates the objects captured by the appropriate means, and then secures them.

The investigator must instantly establish a chain of custody for the evidence. The objects need to be labelled and placed into bags or wrapped with tape. The identification information should be written on bags or tap. The CFS is aware of the need to be careful about the type of bag to use. For example, soft bags would be needed for certain types of devices to prevent accidental alteration of the evidence. The CFS also needs to immediately record all items of evidence on a chain of custody form designed for cyber forensic investigations.

Subsequently, the CFS would transport the original evidence to a secure forensics lab, where a closet or locker is used to store the original evidence securely. The laboratory has the tools and equipment necessary to perform the appropriate tests and procedures. Sometimes the CFS will need to obtain digital images on site when circumstances may prevent the equipment from being moved to the laboratory.

The CFS should make copies of the original without interfering with or altering the originals because the CFS cannot perform tests or procedures on the original objects. The CFS takes the originals one by one and makes working copies from which tests will be performed. Streaming software is needed for hard drives to make sure the working copy is an exact duplication of the original because of concealed digital evidence that would not get copied with normal copy procedures. The CFS, during this process, would need to validate the copies as being exact duplicates before performing any tests.

At that point, the CFS needs a strategy of precisely what tests and procedures to perform. If that plan was not created in advance, it should be properly documented at this step. This would include the tests, tools, objectives and techniques. Then the CFS implements the plan, using suitable documents, tools and any evidence extracted.

Courts and judges want to see expertise used in handling evidence presented to the court. Part of that would be evidence that the expert used formal procedures, such as a checklist, and industry standard best practices in handling data, extracting data, and analysing data, just like courts do with valuation experts and other experts.

As a final point, the CFS takes the examination and conclusions and turns the digital data into functional, effective objects for the main investigator, attorneys, and especially for the court, if applicable (i.e. judge and/or jury). Typically, that would be useful graphs, a slide show file or plain English, to ease the ability of a reader to assimilate the facts without intellectual terms, highly technical graphs or scholarly discussions. The CFS may obviously be called as an expert witness if a trial becomes essential.

### Variety of Experts in Cyber Forensics

A CFS is an SME (subject matter expert) with a particular set of skills, knowledge, and abilities. The cyber forensics profession; however, has a variety of experts within it. There are a minimum of three different experts that it uses:

- Computer investigator (Internet, networks, locating computer communications)
- Digital evidence collection expert (hold and preserve digital evidence)
- Computer forensic auditor (withdraws data for investigators)

This list demonstrates the need to know different types of cyber forensic specialists, and the probability of the need for several CFS on an investigative team, and it also demonstrates that the whole cyber forensic world is really complicated.

## Suggested Further Readings:


- ✓ Saurav K. Dutta; Published Jun 18, 2013 : Statistical Techniques for Forensic Accounting: Understanding the Theory and Application of Data Analysis
- ✓ Golden, T.W., Skalak, S., Clayton, M. (2006) A Guide to Forensic Accounting Investigation
- ✓ Albrecht, C.C., Albrecht, W. (2005) Fraud Examination
- ✓ Brown, A., Doig, A., Summers, G., Dobbs, L. (2004) Practically Fraud