INTRODUCTION TO COMPUTER FORENSICS

1. INTRODUCTION TO TRADITIONAL COMPUTER CRIME

##### Computer Crime

Computers can be involved in a wide variety of crimes including white-collar crimes, violent crimes such as murder and terrorism, counterintelligence, eco- nomic espionage, counterfeiting, and drug dealing. The Internet has made targets much more accessible, and the risks involved for the criminal are much lower than with traditional crime.

A computer can play one **of three roles in a computer crime**.

computer can be the target of the crime

it can be the instrument of the crime,

it can serve as an evi- dence repository storing valuable information about the crime

For example, a hacker may use the computer as the tool to break into another computer and steal files, then store them on the computer. When investigating a case, it is important to know what roles the computer played in the crime and then tailor the investigative process to that particular role.

If the computer was used to hack into a network password file, the investigator will know to look for password cracking software and password files. If the computer was the target of the crime, such as an intrusion, audit logs and unfamiliar programs should be checked

**The Computer Forensic Objective**

The objective in computer forensics is quite straightforward. It is to recover, analyze, and present computer-based material in such a way that it is useable as evidence in a court of law. The key phrase here is *useable as evidence in a court of law*. It is essential that none of the equipment or procedures used during the examination of the computer obviate this.

**The Computer Forensic Priority**

Computer forensics is concerned primarily with forensic procedures, rules of evi- dence, and legal processes. It is only secondarily concerned with computers. There- fore, in contrast to all other areas of computing, where speed is the main concern, in computer forensics the absolute priority is accuracy. One talks of completing work as efficiently as possible, that is, as fast as possible without sacrificing accuracy.

# Lack of Reporting

Although estimates vary, most experts agree that the vast majority of Fortune 500 companies have been electronically compromised to the tune of at least $10 bil- lion/year. However, early studies indicated that only 17 percent of such victim- izations were reported to law enforcement authorities (Center for Strategic and International Studies, 1998). At the same time, number of reported incidents handled by Carnegie-Mellon University (CERT–Computer Emergency Response Team) has increased from 1,334 in 1993 to 4,398 during the first two quarters of 1999 (U.S. General Accounting Office, **1998). It does appear that reporting is get- ting better; a survey of 521 security personnel from American companies, financial institutions, universities and governme**nt agencies revealed that 32 percent of respondents reported electronic crime to law enforcement. This represented an increase of 15 percent of the previous study. However, computer intrusion is still vastly underreported.

# 1.1 TRADITIONAL PROBLEMS ASSOCIATED WITH COMPUTER CRIME

Individuals seeking a crime have always displayed a remarkable ability to adapt to changing technologies, environments, and lifestyles. This adaptability has often placed law enforcement at a disadvantage, struggling to keep up with criminal innovations. This trend has proven to be true in contemporary society. Fortunately, much computer-related crime involves non-specialist users (e.g., child pornography, drug dealers, harassment, etc.). In fact, the earliest computer crimes were characterized as non-technological specific. Theft of computer components and software piracy were particular favorites. Hacking and technologically complicated computer crime came later.

Although the advent of technology has vastly changed the modus operandi of certain criminal elements throughout history, current advances have changed the very physical environment in which crime occurs. As such, the law enforcement community has experienced unprecedented periods of uncertainty and ineffec- tiveness. Many of these problems are associated with the comprehension of the nature of the emerging technology, while others involve questions of legality and sovereignty. Unfortunately, legislative bodies and judicial authorities have been slow to respond to such inquiries, and law enforcement has been forced to de- velop investigative techniques without adequate legal foundations. At the same time, the lack of technological knowledge traditionally associated with the law enforcement community hampers even the most mundane investigation. So, while the investigators of computer-related crime must display the levels of ingenuity comparable to sophisticated criminal entrepreneurs, traditional investigators are ill-equipped to do so.

# Physicality and Jurisdictional Concerns:

The physical environment that breeds computer crime is far different from tradi- tional venues. In fact, the intangible nature of computer interaction and subse- quent criminality poses significant questions for investigative agents. For exam- ple, what forensic tools are available for identifying entry points in data breaking and entering? Certainly, seasoned investigators recognize the utility of prymark analysis in home burglaries. But few recognize the how-to’s and what-for’s in ab- stract, intangible environments. In many cases, such differences in technique, and even approach, are further complicated by the lack of precautionary boundaries and restraints—both physical and virtual. Indeed, the intangibility of such envi- ronments creates unlimited opportunities.

The lack of physical boundaries and the removal of traditional jurisdictional demarcations allow perpetrators to commit multinational crime with little fear (or potential) of judicial sanctions. For the first time, criminals can cross international boundaries without the use of passports or official documentation. Whereas tra- ditional criminal activity required the physical presence of the perpetrators, cy- bercrime is facilitated by international connections that enable individuals to com- mit criminal activity in England while sitting in their offices in Alabama. In addition, electronic crime does not require an extensive array of equipment or tools. It does not require vehicular transportation, physical storage capability, or labor-intensive practices, all of which increase the potential for discovery and en- forcement. In addition, this shift from a corporeal environment, where items can be seen, touched, smelled, etc., to a virtual world where boundaries, concrete bar- riers and physical items are inconsequential, has further insulated the criminal from law enforcement. In fact, the sheer intangibility of crime scenes has all but crippled many criminal investigations.

A further concern regarding the physical intangibility of computer crime in- volves the traditional lack of cooperation inherent in law enforcement investiga- tions. Issues of funding, political platforms, and the like have traditionally reduced communication and cooperation among jurisdictions. These issues are further compounded when international components are considered. The lack of con- sensus among international entities regarding the criminalization of certain behav- iors and the appropriate sanctions associated with same often negate cooperative agreements.

# Perceived Insignificance and Stereotypes:

Investigators and administrators have displayed great reluctance to pursue computer criminals. A lack of knowledge coupled with general apathy towards cyber- criminality has resulted in an atmosphere of indifference. Many stereotype computer criminals as non-threatening, socially challenged individuals (i.e., nerds or geeks), and fail to see the insidious nature of computer crime. The potentiality of weapons and narcotics trafficking, conspiracies of mass destruction, and the like are all but alien to those individuals not actively involved in computer investigations. In addition, those administrators and investigators who grudgingly admit the presence and danger of electronic crime tend to concentrate exclusively on child pornography, overlooking motivations and criminal behaviors apart from sexual gratification. Unfortunately, these perceptions are often directly opposed to the reality experienced by seasoned investigators.

# Lack of Reporting:

Although estimates vary, most experts agree that the vast majority of Fortune 500 companies have been electronically compromised to the tune of at least $10 bil- lion/year. However, early studies indicated that only 17 percent of such victim- izations were reported to law enforcement authorities (Center for Strategic and International Studies, 1998). At the same time, number of reported incidents handled by Carnegie-Mellon University (CERT–Computer Emergency Response Team) has increased from 1,334 in 1993 to 4,398 during the first two quarters of 1999 (U.S. General Accounting Office, 1998). It does appear that reporting is get- ting better; a survey of 521 security personnel from American companies, finan- cial institutions, universities and government agencies revealed that 32 percent of respondents reported electronic crime to law enforcement. This represented an increase of 15 percent of the previous study. However, computer intrusion is still vastly underreported.

# Lack of Resources:

Although computer intrusions have proven to be problematic within the corpo- rate world, their unwillingness or inability to effectively communicate with judi- cial authorities has led to an increase in computer crime. Unfortunately, law en- forcement and corporate entities desperately need to cooperate with one another. Unlike their civil service counterparts, the business communities have the re- sources (both financial and legal) necessary to effectively combat computer crimes. First, these companies, through their system administrators, have far more leeway in monitoring communications and system activities, and they have the ability to establish policies which enable wide-scale oversight.

# Jurisprudential Inconsistency:

Unfortunately, the Supreme Court has remained resolutely averse to deciding mat- ters of law in the newly emerging sphere of cyberspace. They have virtually de- nied cert on every computer privacy case to which individuals have appealed, and have refused to determine appropriate levels of Fourth Amendment protections of individuals and computer equipment. As such, the country is remarkably di- vided on fundamental elements of law—establishing a legality standard of be- havior in one jurisdiction which negates or supersedes another.

2 INTRODUCTION TO IDENTITY THEFT & IDENTITY

## 2.1 Identity Fraud

### A typology of ID change

Identity fraud can roughly be described as the unlawful changing of someone’s iden- tity. Rost, Meints, and Hansen [Le06:52-55, RoMe05] distinguish four closely related subcategories of identity change:

* identity takeover, when someone takes over the identity of another person with- out that person’s consent;
* identity delegation, when someone uses someone else’s identity with that per- son’s consent;
* identity exchange, when two or more people, with mutual consent, use each other’s identity;
* identity creation, when someone creates the identity of a non-existing person.

In all subtypes, the identity change can be perfectly lawful. For instance, a Tony Blair doppelgänger can walk the streets of Lon- don to see how the public reacts; a wife can lend her bank card to her husband to pur- chase something; the prince and the pauper can swap lives for a day; and Eric Arthur Blair may well choose a pseudonym to publish his books. Nevertheless, many cases of identity change can be considered unlaw- ful. When the Tony Blair look-alike uses his doppelgängsterism to receive free services or goods, he commits fraud, and when a director gives the password to her digital signature to her secretary to sign documents he is not authorised to sign, she also com- mits fraud. Swapping loyalty cards to thwart a supermarket’s profiling will not generally be considered fraud, but – de- pending on the terms and conditions – may well constitute tort. And using a self- generated credit-card number that fulfils the characteristics of credit-card numbers clearly is unlawful.As these examples already illustrate, the bulk of identity fraud cases will readily fall within the ambit of the traditional notion of fraud. This means that, from a strictly legal perspective, there is no need to pay specific attention to identity-related fraud: most if not all cases can be prosecuted as fraud.

Why, then, should we handle identity fraud as a separate category of crime? Al-though it is not a foregone conclusion that identity fraud is an intrinsic category in its own right, we feel that it merits special treatment, for several reasons. First and foremost, fraud occurs in forms and on a scale formerly unknown, because of the new role of identity management in the information society. Face-to-face transac- tions have increasingly given way to e- commerce and on-line service-provision, and the information society is based on an ever more complex web of interactions in intricately interwoven relationships. This implies that identifiers such as names and numbers have become much more impotant as essential entry points for social interactions: without ID, nothing happens – at least nothing much that is legally releant. (We use ‘ID’ here in the sense of a partial identifier, which may also be pseudonymous.) And along with the new role of identity in the information society, identity fraud is emerging as an unavoidable consequence.

A comparison with computer-related crime may be instructive here. Although computer fraud can be conceived of as simply another means to commit fraud, it has been considered a category in its own right since the 1980s, when computers started fundamentally changing the way in which society functions. As a result, from the OECD’s 1986 report Computer-related Crime to art. 8 of the 2001 Convention on Cybercrime, computer-related fraud has featured prominently in instruments to combat computer crime. This is not primar- ily because forms of computer fraud were not punishable under traditional criminal provisions such as fraud or forgery, al- though there certainly were some legislative gaps. Rather, specific attention and crimi- nalisation were warranted because combat- ing computer fraud requires special knowl- edge of computers. Investigation and prose- cuting computer fraud implies that the police and judiciary know how to investi- gate and judge the technical odds and ends of computers and computer data. Moreover, successfully combating computer fraud is not only a matter of prosecution, but also – and perhaps even more – a matter of pre- vention. For this, awareness must be raised, since computers create specific vulnerabili- ties that organisations and individuals tend to disregard through ignorance.

A significant part of any identity-fraud combating strategy is awareness-raising. This is a second reason to treat identity fraud as a special category. Opportunities for identity fraud thrive as long as people develop and use identity-management technologies without heed of their potential for abuse. It is only when people are edu- cated about the various risks of identity fraud, that the weakest link in identification vulnerabilities can be strengthened. In this respect, Europe can benefit from the exam- ple of the US, where through the Identity Theft and Assumption Deterrence Act, a complaint and education centre has been established with the Federal Trade Commis- sion.3 In Europe, the UK has a similar web- site.4

A third reason to look at identity fraud as a separate category is the victim’s perspec- tive. Unlawful identity takeover (‘identity theft’) differs from traditional fraud in two fundamental ways. First, it takes time for the victim to notice the crime, which may happen long after the identity ‘thief’ has fled to Vanuatu with his gains. Second, the victimisation of the victim may well con- tinue long after the crime, since, contrary to most traditional cases of fraud, a feature of identity takeover is that the victim is black- listed and has difficulty in regaining her credit history and trustworthy image. This difficulty is another characteristic of current identification infrastructures. It is therefore altogether important to study the specifics of identity fraud in order to support victims effectively.

## 2.2 Identity Theft

Having focused on identity fraud as a useful target of research, we have still the preva- lent term of ‘identity theft’ to consider. What is usually meant by this term is the subcategory of unlawful identity takeover from the broader category of identity fraud.

‘Identity theft’ is a rather awkward term, since identity is not something that is typi- cally stolen. A characteristic of theft, after all, is that the owner no longer possesses the stolen thing. With identity, this is usually not the case: the victim of identity takeover still retains her identity. We should therefore speak of ‘identity „theft”’ rather than of ‘identity theft’. Another reason to be hesi- tant in using this term broadly, is that it invites overlooking the other forms of identity fraud. The consequences for third parties of identity takeover *with* consent (as in unlawful identity delegation or exchange) may be equally serious as those of identity takeover without consent (as in identity ‘theft’). Policy-making and action plans should therefore not be confined to uncon- sensual identity takeover.

Having said this, we admit that identity ‘theft’ is a major issue and probably the most important subset of identity fraud and identity-related crime at large. Giving a definition is, however, not straightforward. The definitions in section 1 focus on the assumption or use of the identity of another existing person. As in our discussion of identity fraud, it is questionable whether this strikes the right note. By focusing only on the element of another’s identity, it is implied that the crime is targeted at the person whose identity is taken. Mitchison’s description explicitly calls this person ‘the victim’ of the crime. However, from the perspective of the perpetrator, the target is not so much the identity bearer as the per- son or institution who is fooled by the false identity. The latter may equally truly be called a victim of the crime. Again, it seems a matter of focusing on the preparatory act of assuming a false identity as such versus focusing on committing a crime by using a false identity. The former has, almost by definition, the identity bearer as victim. In the latter approach, the victim of the crime is the one who bears the loss; depending on the allocation of liabilities in the legal sys- tem, this may be the shop or institution who provides goods or services to the wrong person, the bank accepting the means of payment, and/or the person in whose name the transaction is being done and who may be blacklisted as a result. This is context- dependent.

Since identity ‘theft’ is not primarily tar- geted at the person whose identity is used, and since the question who is the victim of the crime depends on the context of the modus operandi and the legal distribution of liabilities, we propose to stress the ‘target crime’ – usually fraud, and occasionally other crimes such as slander or extortion – rather than the subsidiary element of using another’s identity. The latter element is nevertheless relevant, from the perspective of awareness and the grave consequences for identity bearers if they *are* victims. This leads to the following definition.

Identity ‘theft’ is fraud or another unlaw- ful activity where the identity of an ex- isting person is used as a target or prin- cipal tool without that person’s consent.

3.TYPES OF CF TECHNIQUES

# 3.1 Modern Forensic Science Technologies

  1. [Laser Ablation Inductively Coupled Plasma Mass Spectrometry (LA-ICP-MS)](https://www.ncjrs.gov/pdffiles1/nij/grants/232134.pdf) : When broken glass is involved in a crime, putting together even tiny pieces can be key to finding important clues like the direction of bullets, the force of impact or the type of weapon used in a crime. Through its highly sensitive isotopic recognition ability, the LA-ICP-MS machine breaks glass samples of almost any size down to their atomic structure. Then, forensic scientists are able to match even the smallest shard of glass found on clothing to a glass sample from a crime scene. In order to work with this type of equipment in conjunction with forensic investigation, a Bachelor’s Degree in Forensic Science is usually necessary.

      2.    [Alternative Light Photography](http://books.google.com/books?id=mpxTRdbspWEC&pg=PA146&lpg=PA146&dq=alternative+light+photography+forensic+nursing) : For a forensic nurse, being able to quickly ascertain how much physical damage a patient has suffered can be the difference between life and death. Although they have many tools at their disposal to help make these calls quickly and accurately, Alternative Light Photography is one of the coolest tools to help see damage even before it is visible on the skin. A camera such as the Omnichrome uses blue light and orange filters to clearly show bruising below the skin’s surface. In order to use this equipment, you would need a MSN in Forensic Nursing.

      3. [High-Speed Ballistics Photography](http://books.google.com/books?id=cf9nMdmTrNIC&pg=PA330&dq=high+speed+photography+forensics) : You might not think of it right away as a tool for forensic scientists, but ballistics specialists often use high-speed cameras in order to understand how bullet holes, gunshot wounds and glass shatters are created. Virtually anyone, from a crime scene investigator to a firearms examiner, can operate a high-speed camera without any additional education or training. Being able to identify and match bullet trajectories, impact marks and exit wounds must be done by someone with at least a Bachelor’s of Science in Forensic Science.

      4. [Video Spectral Comparator 2000](http://www.safde.org/whatwedo.htm) : For crime scene investigators and forensic scientists, this is one of the most valuable forensic technologies available anywhere. With this machine, scientists and investigators can look at a piece of paper and see obscured or hidden writing, determine quality of paper and origin and “lift” indented writing. It is sometimes possible to complete these analyses even after a piece of paper has been so damaged by water or fire that it looks unintelligible to the naked eye. In order to run this equipment, at least a Bachelors degree in Forensic Science or a Master’s Degree in Document Analysis is usually required

      5. [Digital Surveillance For Xbox (XFT Device)](http://www.sciencedaily.com/releases/2009/04/090430101445.htm) : Most people don’t consider a gaming system a potential place for hiding illicit data, which is why criminals have come to use them so much. In one of the most ground-breaking forensic technologies for digital forensic specialists, the XFT is being developed to allow authorities visual access to hidden files on the Xbox hard drive. The XFT is also set up to record access sessions to be replayed in real time during court hearings. In order to be able to access and interpret this device, a Bachelor’s Degree in Computer Forensics is necessary.

      6. 3D Forensic Facial Reconstruction : Although this forensic technology is not considered the most reliable, it is definitely one of the most interesting available to forensic pathologists, forensic anthropologists and forensic scientists. In this technique, 3D facial reconstruction software takes a real-life human remains and extrapolates a possible physical appearance. In order to run this type of program, you should have a Bachelor’s Degree in Forensic Science, a Master’s Degree in Forensic Anthropology or a Medical Degree with an emphasis on Forensic Examination and Pathology.

      7. [DNA Sequencer](http://www.ndaa.org/pdf/forensic_dna_fundamentals.pdf) : Most people are familiar with the importance of DNA testing in the forensic science lab. Still, most people don’t know exactly what DNA sequencers are and how they may be used. Most forensic scientists and crime lab technicians use what’s called DNA profiling to identify criminals and victims using trace evidence like hair or skin samples. In cases where those samples are highly degraded, however, they often turn to the more powerful DNA sequencer, which allows them to analyze old bones or teeth to determine the specific ordering of a person’s DNA nucleobases, and generate a “read” or a unique DNA pattern that can help identify that person as a possible suspect or criminal.

      8. [Forensic Carbon-14 Dating](http://www.nij.gov/journals/269/pages/carbon-dating.aspx) : Carbon dating has long been used to identify the age of unknown remains for anthropological and archaeological findings. Since the amount of radiocarbon (which is calculated in a Carbon-14 dating) has increased and decreased to distinct levels over the past 50 years, it is now possible to use this technique to identify forensic remains using this same tool. The only people in the forensic science field that have ready access to Carbon-14 Dating equipment are forensic scientists, usually with a Master’s Degree in Forensic Anthropology or Forensic Archaeology.

      9. [Magnetic Fingerprinting and Automated Fingerprint Identification (AFIS)](http://searchsecurity.techtarget.com/definition/Automated-Fingerprint-Identification-System) : With these forensic technologies, crime scene investigators, forensic scientists and police officers can quickly and easily compare a fingerprint at a crime scene with an extensive virtual database. In addition, the incorporation of magnetic fingerprinting dust and no-touch wanding allows investigators to get a perfect impression of fingerprints at a crime scene without contamination. While using AFIS requires only an Associates Degree in Law Enforcement, magnetic fingerprinting usually requires a Bachelor’s Degree in Forensic Science or Crime Scene Investigation.

      10. [Link Analysis Software for Forensic Accountants](http://www.theifp.org/research-grants/IFP-Whitepaper-4.pdf) : When a forensic accountant is trying to track illicit funds through a sea of paperwork, link analysis software is an invaluable tool to help highlight strange financial activity. This software combines observations of unusual digital financial transactions, customer profiling and statistics to generate probabilities of illegal behavior. In order to accurately understand and interpret findings with this forensic technology, a Master’s Degree in Forensic Accounting is necessary.

# 3.2 A Military Cyber Forensics Definition

Given the above considerations, we offer the following definition for cyber forensics. “*The exploration and application of scientifically proven methods to gather, process,interpret, and utilize digital evidence in order to:*

* *Provide a conclusive description of all cyber-attack activities for the purpose of complete post-attack enterprise and critical infrastructure information restoration*
* *Correlate, interpret, and predict adversarial actions and their impact on planned military operations*
* *Make digital data suitable and persuasive for introduction into a criminal investigative process”*

While the last goal of the definition directly addresses law enforcement needs in cyber forensics, it is also required for the military commander who will be making decisions on how to engage aggressors in cyberspace, who may be civilian enemy combatants rather than state-sponsored attackers. The commander will need to know for sure who is attacking prior to taking any action that would be viewed as a violation of a Treaty or other international agreement. Forensic results that meet criminal investigative criteria can help justify a commander’s actions in retaliation.

3.3 CRIMINAL JUSTICE: LAW ENFORCEMENT TECHNOLOGY (BS) PROGRAM OUTCOMES:

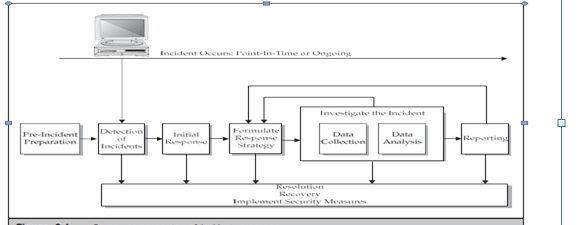
* Graduates will have knowledge of criminal investigations and criminalistics and be able to analyze the elements that constitute crimes and effectively apply scientific methods towards crime scene investigations.
* Graduates will have knowledge of the technologies used in a variety of criminal justice and law enforcement applications ranging from crime scene investigations to digital forensic investigations.
* Graduates will gain competencies in evidence collection, documentation, analysis and maintenance of chain of custody as well as the laws and guidelines associated with these matters.
* Graduates will take specialized courses to gain knowledge in areas such as geographical information systems, crime analysis and prevention, security, and law enforcement technologies.

# 4.INCIDENT & INCIDENT RESPONSE METHODOLOGY

We are always on a quest for the perfect way to organize a process. We search for the right way to define phases of the process, look for bright-line separation of phases to avoid murky areas, try to make the perfect flowchart to illustrate the process, and organize the phases so the process can be applied to the widest range of possible scenarios. Since the incident response process can involve so many variables and factors that affect its flow, it is quite a challenge to create a simple picture of the process while maintaining a useful level of accuracy. However, we feel that we have developed an incident response process that is both simple and accurate.

Computer security incidents are often complex, multifaceted problems. Just as with any complex engineering problem, we use a “black box” approach. We divide the larger problem of incident resolution into components and examine the inputs and outputs of each component. Figure 2-1 illustrates our approach to incident response. In our method- ology, there are seven major components of incident response:

▼Pre-incident preparation Take actions to prepare the organization and the CSIRT before an incident occur



Detection of incidents Identify a potential computer security incident.

* Initial response Perform an initial investigation, recording the basic details surrounding the incident, assembling the incident response team, and notifying the individuals who need to know about the incident.
* Formulate response strategy Based on the results of all the known facts, determine the best response and obtain management approval. Determine what civil, criminal, administrative, or other actions are appropriate to take, based on the conclusions drawn from the investigation.
* Investigate the incident Perform a thorough collection of data. Review the data collected to determine what happened, when it happened, who did it, and how it can be prevented in the future.
* Reporting Accurately report information about the investigation in a manner useful to decision makers.

▲ Resolution Employ security measures and procedural changes, record lessons learned, and develop long-term fixes for any problems identified.

# 4.1 WHAT ARE THE GOALS OF INCIDENT RESPONSE?

In our incident response methodology, we emphasize the goals of corporate security pro- fessionals with legitimate business concerns, but we also take into consideration the con- cerns of law enforcement officials. Thus, we developed a methodology that promotes a coordinated, cohesive response and achieves the following:

▼ Prevents a disjointed, noncohesive response (which could be disastrous)

* Confirms or dispels whether an incident occurred
* Promotes accumulation of accurate information
* Establishes controls for proper retrieval and handling of evidence
* Protects privacy rights established by law and policy
* Minimizes disruption to business and network operations
* Allows for criminal or civil action against perpetrators
* Provides accurate reports and useful recommendations
* Provides rapid detection and containment
* Minimizes exposure and compromise of proprietary data
* Protects your organization’s reputation and assets
* Educates senior management

▲ Promotes rapid detection and/or prevention of such incidents in the future (via lessons learned, policy changes, and so on)

# 4.2 WHO IS INVOLVED IN THE INCIDENT RESPONSE PROCESS?

Incident response is a multifaceted discipline. It demands a myriad of capabilities that usually require resources from several different operational units of an organization. Hu- man resources personnel, legal counsel, technical experts, security professionals, corpo- rate security officers, business managers, end users, help desk workers, and other employees may find themselves involved in responding to a computer security incident.

Most organizations establish a team of individuals, often referred to as a *Computer Security Incident Response Team* (*CSIRT*), to respond to any computer security incident. The CSIRT is a multidisciplined team with the appropriate legal, technical, and other expertise necessary to resolve an incident. Since the CSIRT members have special exper- tise, and incident response is not required at all times, the CSIRT is normally a dynamic team assembled when an organization requires its capabilities.

### INVESTIGATION PROCESS

The number of suggested and proposed investigation models is not small, as such, it would be quite a daunting exercise to review them all. We have indeed, selected the models to be reviewed based on the chronological order, ensuring at least one proposed model per year. We are not suggesting that the selected models are better or superior than the other models that were also introduced in the same year. Our objective is to identify and extract the phases in the investigation models rather than selecting which model is the best.

# Computer Forensic Investigative Process (1984)

Pollitt [2] [3] has proposed a methodology for dealing with digital evidence investigation so that the results with be scientifically reliable and legally acceptable. It comprises of 4 distinct phases.

Acquisition Identification Evaluation Admission

Figure 1: Computer Forensic Investigative Process

In Acquisition phase, evidence was acquired in acceptable manner with proper approval from authority. It is followed by Identification phase whereby the tasks to identify the digital components from the acquired evidence and converting it to the format understood by human. The Evaluation phase comprise of the task to determine whether the components indentified in the previous phase, is indeed relevant to the case being investigated and can be considered as a legitimate evidence. In the final phase, Admission, the acquired & extracted evidence is presented in the court of law.

* 1. Generic Computer Forensic Investigation Model (GCFIM)

Phase 1 of GCFIM is known as *Pre-Process*. The tasks performed in this phase relates to all of the works that need to be done prior to the actual investigation and official collection of data. Among the tasks to be performed are getting the necessary approval from relevant authority, preparing and setting-up of the tools to be used, etc.

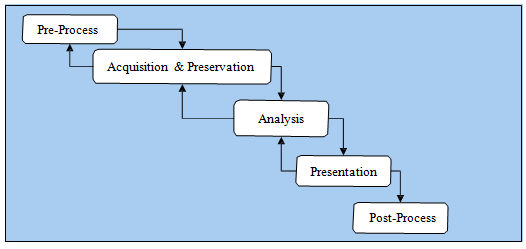
Phase 2 is known as *Acquisition & Preservation*. Tasks performed under this phase related to the identifying, acquiring, collecting, transporting, storing and preserving of data. In general, this phase is where all relevant data are captured, stored and be made available for the next phase.

Phase 3 is known as *Analysis*. This is the main and the center of the computer forensic investigation processes. It has the most number of phases in its group thus reflecting the focus of most models reviewed are indeed on the analysis phase Various types of analysis are performed on the acquired data to identify the source of crime and ultimately discovering the person responsible of the crime.

Phase 4 is known as *Presentation*. The finding from analysis phase are documented and presented to the authority. Obviously, this phase is crucial as the case must not only be presented in a manner well understood by the party presented to, it must also be supported with adequate and acceptable evidence. The main output of this phase is either to prove or refute the alleged criminal acts

Phase 5 is known as *Post-Process*. This phase relates to the proper closing of the investigation exercise. Digital and physical evidence need to be properly returned to the rightful owner and kept in safe place, if necessary. Review of the investigative process should be done so that the lesson can be learnt and used for improvement of the future investigations.

Instead of moving sequentially from one phase to another, the ability to go back to the previous phases must always be present. We are dealing with the situations that are forever changing in terms of the crimes scenes (physical and digital), the investigative tools used, the crime t used and the level of expertise for the investigators. As such, it is much desired to be able to go back to the previous phases that we have done, not only to correct any weaknesses but also to acquire new things/information.



5.3 Forensic Duplications

* A forensic duplication means to make a complete, byte-by-byte copy of the contents of a storage device
* The goal is to transfer all data from the suspect system to the forensic copy without altering the suspect system in any way Special devices that block writing operations to the suspect system is used

## Preparation FOR IR

### 6.1 Incident Response Team

In any organisation, an Incident Response Team (“IRT”) should be made up of senior management and experienced people. The role of the IRT is to promptly handle an incident so that containment, investigation and recovery can quickly occur. The IRT should be empowered by the top management to have decision-making authority for facilitating the incident response process. The needs and resources of the company also play a part in the selection of the team members. The table below shows a list of members who should be included in the IRT and their roles in the team.

|  |  |  |
| --- | --- | --- |
| No. | IRT Member | Role in IRT |
| 1. | Senior Management | Apart from providing the team the authority for operation, the management has to make business-related decisions based on input from the other members of the team. |
| 2. | Information Security | Assess the extent of the damage incurred and perform containment, basic forensics, and recovery. |
| 3. | IT/MIS | Minimise the impact to system end users, and to assist the Information Security team with technical issues. |
| 4. | IT Auditor | Understand the cause of the incident, ensure procedures are complied with, and work with IT/Security to eradicate the incident. |
| 5. | Security | Assess physical damage incurred, investigate physical evidence, and guard evidence during a forensics investigation to maintain a chain of evidence. |
| 6. | Legal | Ensure the usability of any evidence collected during an investigation if the company chooses to take legal action. The role also includes providing advice regarding liability issues in the event that an incident affects customers, vendors, and/or the general public. |
| 7. | Human Resource | Provide advice in situations involving employees. HR will only be involved in handling the incident if an employee is found to be responsible for the intrusion. |
| 8. | Public Relations | Communicate with team leaders to have an accurate understanding of the issue and the company’s status before communicating with the press and/or informing the stockholders of the current situation. |
| 9. | Financial Auditor | Assess the damage incurred in terms of monetary value, which is frequently required for insurance companies or if the company intends to press charges against the perpetrator. |

For small and medium sized merchants/processors one person may assume one or more of these responsibilities. An external party/consultant may also assume one e.g. public relations.

### IRT structure

Within the IRT, further division into three sub-teams: the Supervisory Team, the Site Team and the Support Team, may be formed based on the roles of the team members.

Table 2: Members in each IRT sub-team

|  |  |  |
| --- | --- | --- |
| Supervisory Team | Site Team | Support Team |
| Senior Management | IT/MIS | Human Resource |
| Information Security | Security | Public Relations |
| IT Auditor | IT Auditor | Legal |
| Financial Auditor |  |  |

The following diagram illustrates an overview of the team structure in IRT:

**Supervisory Team**

**Site Team**

**Network Operations**

**Virus Alert Team**

**IT Helpdesk**

**IRT Leader**

**Support Team**

Examples of extended technical

support team (engaged as needed)

The responsibility of the Supervisory Team includes:

1. making decisions on, and reviewing steps taken to rectify matters
2. communicating and translating technical information to senior management or board of directors
3. supervising and reviewing test results based on the tests conducted to verify the feasibility and effectiveness of the incident response procedures
4. cooperating with and supplying information to the support team so that their duties can be carried out
5. coordinating resources, e.g. software and hardware acquisition, if required
6. maintaining proper records of events and actions taken
7. attending, establishing and conducting training for relevant personnel
8. performing scenario planning and identifying corrective actions for each scenario; and
9. supervising and reviewing the update, including lessons learnt, on the Incident Response Procedures.

The responsibility of the Site Team includes:

1. surveying and securing the systems and environment
2. containing the incident
3. eradicating incident and performing recovery procedures
4. compiling “recovery kit”, e.g. recovery procedures, contact list, boot disks, software, tools, hard disk, and so on
5. attending and conducting training for relevant personnel and
6. updating and maintaining the Incident Response Procedures. The responsibility of the Support Team includes:
7. providing logistic and technical support to other IRT teams when required
8. updating public and relevant authorities via commercial press, web sites, telephone and others, and
9. coordinating communications for the company with various external parties, if required.

A leader will be appointed in the IRT as the point of contact in the event of an incident. When an incident is reported by the helpdesk, the leader will be responsible for contacting the relevant sub-teams to handle the incident (refer to Appendix E for a detailed incident response work process).

A contact list for IRT members and external parties (for both office and non-office hours) should be developed and made available to the team (refer to Appendix A for the Incident Response Contact List).

When reporting the incident, communication should be made via the telephone and/or fax machine. This is to prevent interception of emails by the perpetrator if the computer used for sending the email has been compromised or by a “sniffer” program that has been planted on the network to capture information sent across the network. Should sensitive electronic media need to be passed to a third party (e.g. listings of account numbers that were leaked) this may be done via secure courier. However the media must be strongly encrypted.

Depending on situation, support from other technical teams in the Company (e.g. the network operations, anti-virus team or IT helpdesk) may be required to assist in the incident handling process.

7.FORENSICS TECHNOLOGY AND SYSTEMS

computer forensics has become a buzz word in today’s world of increased concern for security. It seems that any product that can remotely be tied to network or computer security is quickly labeled as a “forensics” system. This phenomenon makes designing clear incident response plans and corporate security plans that support computer forensics difficult.This chapter is intended to raise awareness of the different types of computer forensics systems and to identify crucial questions for corporate planning in support of computer forensics.

* Internet security systems
* Intrusion detection systems
* Firewall security systems
* Storage area network security systems
* Network disaster recovery systems
* Public key infrastructure security systems
* Wireless network security systems
* Satellite encryption security systems
* Instant messaging (IM) security systems
* Net privacy systems
* Identity management security systems
* Identity theft prevention systems
* Biometric security systems
* Homeland security systems

Understanding Computer Investigations:

* When preparing a case, you can apply standard systems analysis steps to problem solving,which are explained in the following list. Make an initial assessment about the type of case you are investigating : Determine the resources you need: Based on the OS of the computer you’re investigating, list the software you plan to use for the investigation, noting any other software or tools you might need.Obtain and copy an evidence disk drive In some cases, you might be seizing multiple computers along with Zip disks, Jaz drives, CDs, thumb drives, PDAs, and other removable media
* Identify the risks: List the problems you normally expect in the type of case you are handling. This list is known as a standard risk assessment. Mitigate or minimize the risks: Identify how you can minimize the risks.
* Test the design: Review the decisions you’ve made and the steps you’ve already completed.
* Analyze and recover the digital evidence: Using the software tools and other resources gathered, and overcoming the risks and obstacles you identified, examine the disk to find digital evidence. Investigate the data you recover:
* Critique the case: Self-evaluation is a critical part of professional growth.

7.1 Planning Your Investigation

* Now that you have identified the requirements of the Domain Name case, you can plan your investigation. You have already determined the kind of evidence you need; now you can identify the specific steps to gather the evidence, establish a chain of custody, and perform the forensic analysis.

1. Acquire the floppy disk from George’s manager.

2. Complete an evidence form and establish a chain of custody.

3. Transport the evidence to your computer forensics lab.

4. Secure your evidence in an approved secure container.

5. Prepare your forensic workstation.

6. Obtain the evidence from the secure evidence container.

7. Make a forensic copy of the evidence floppy disk.

8. Return the evidence floppy disk to the secure evidence container.

9. Process the copied floppy disk with your computer forensics tools.