Cyber-Criminal Activity and Analysis

White Paper
Fall 2005

Group 2

Nilkund Aseef (naseef@microsoft.com)
Pamela Davis (pdavis@berkeley.edu)
Manish Mittal (manishm@microsoft.com)
Khaled Sedky (khaleds@microsoft.com)
Ahmed Tolba (ahmedt@microsoft.com)

A teenager in Massachusetts makes a bomb threat to a high school. Following standard procedure, the school closes for two days and has to call in the fire department, Emergency Medical Services, and law enforcement, complete with bomb squad and canine team, to deal with the threat. Months later, the same teenager breaks into a major national phone service provider and steals the personal information of several victims, including the phone numbers of all their friends and family, which the teen then posts on the internet. The teen steals phone service from the company and does the same for several friends, all the while continuing to disrupt operations at the high school through more bomb threats, each of which requires the response of Emergency personnel. When the phone company discovers the theft and shuts down service, the teen issues what appear to be outlandish threats, but not ten minutes after the company refuses to give in, this teen successfully attacks and cripples a significant portion of the provider's business operations.

Over the course of fifteen months, the teen inflicts damages of upwards of one million dollars. When convicted on multiple counts, the teen is sentenced to eleven months' detention and two years' supervised release. During this time, the teen is of course to be kept away from the weapon with which all the above crimes were accomplished: a cell phone. [25]

"Cyber-crime," which refers to any criminal activity committed with the aid of or in the arena of the Internet and similar telecommunications, is both a new incarnation of old crimes through a new medium, and a unique entity all its own. It differs from physical or "terrestrial" crime in four main ways: being easy to commit, requiring minimal resources for great potential damage, being committable in a jurisdiction in which the perpetrator is not physically present,

and often, not being entirely clearly illegal. [24] Virtually any crime, from vandalism to theft, extortion to copyright infringement, can become a cyber-crime.

As new technology often does, cyber-crime also empowers criminals in new ways, such as allowing individuals like this Massachusetts teen to wreak havoc on entities like the telephone company which would previously have been considered far out of their league, but which now are just as vulnerable as anyone to an attacker with the right special abilities and motivation. At the same time, the increased digitalization of all aspects of modern life, from art to government to business, has led to vastly increased stakes and thus increased incentives for cyber-crime.

This paper will examine cyber-crime from a variety of perspectives, starting with a brief history of cyber-crime attacks and corresponding defenses. We will profile some typical attackers, introducing their various skill levels and motivational drivers. In the third section we will address law enforcement, detailing legal and technical procedures involved in cyber-forensics employed to catch cyber-criminals. The fourth section is a guide to current law and policy relating to cyber-crime, and to the limits and problems inherent in this. Finally, we will address current trends, mention common vulnerabilities, and assess the impact of cyber-crime on the economy, consumer trust, the military and national security.

I. History

Rise of cyber-crime:

The early computers like Electronic Numerical Integrator and Computer (ENIAC), Binary Automatic Computer (BINAC), Universal Automatic Computer (UNIVAC), and other punch card tabulation machines had some inherent security advantages. They were standalone systems, huge and very expensive, and besides, not many people knew what a computer really

was. Commercial computers like Programmed Data Processor (PDP-1) got introduced around 1960s with a business model of renting out the machine to companies and individuals on a time sharing basis.[8] This made the data and programs stored in it vulnerable, and thus the first doors to hacking were opened. The first hackers' group came from Massachusetts Institute of Technology (MIT) in 1961, shortly after MIT got its first PDP-1 [8]

During the 1970s, while computers were slowly getting introduced the telephone system was already well established. There was a curious group of people, known as phreaks who thrived by the idea of making free phone calls and looked into various ways of breaking it. One of the first known phreaks was Stewart Nelson from MIT who wrote software to generate tones that helped access the phone company's long distance service and make free calls. The phreaks created a blue box device that was programmed to generate a 2600-hertz signal, allowing them to do nasty things such as stacking a trunk line, and kicking off the operator line that enabled making free long distance calls. Steve Wozniak and Steve Jobs (future founders of Apple Computer) were known to be involved in the early production and distribution of similar devices.

With the introduction of Altair 8800, the first affordable PC in the 1970s it became possible for individuals to own computers and learn to program. This learning was soon followed with a thirst for full-fledged hacking by some individuals. Simultaneously the emergence of other computers like the Radio Shack's TRS-80 and the IBM PC brought more powerful computing to people who were eager to find new ways to exploit the system's capabilities [8]. But these standalone systems limited the potential of damage that could be done once the machine was compromised. It was only with the introduction of networking concepts that the floodgates of hacking were opened. The early networking model consisted of a powerful

mainframe to which many terminals are connected to allow users to share files and run programs. This allowed hackers to access files of other mainframe users and exploit them.

Today's networking technology has improved tremendously, and gone beyond the mainframe model with new concepts such as peer to peer communication. Standards like Ethernet enabled vendors to create compatible products that link computers easily and inexpensively. Interoperability is a key consideration from any business perspective to foster a healthy ecosystem and improve economic growth. Unfortunately, these open standards also made it easier for the hackers to break into systems by reverse engineering the widely available protocols.

As computers became cheaper and started getting mainstream efforts were made for seamless interaction between them. ARPANet was one such effort and during its design, security was not a big issue to research scientists as they thought that the small number of nodes on the network limited the scope of the threat posed by security breaches. However, in 1988, Robert T. Morris, a graduate student at Cornell University launched a self-replicating worm on the government's ARPANet to test its effect on UNIX systems. The worm spread all across the United States, infected thousands of networked computers, clogged government and university systems and brought the Internet to a standstill. This was the wakeup call to Internet users who realized that some amidst them harbored malicious intent.

In early1990s, as Internet access became commercially available at an affordable price, the number of attacks also increased and cyber-crime was now crossing international boundaries. Among the first cyber-espionage case to make international headlines, hackers in West Germany were arrested for breaking into U.S. government and corporate computers, and selling operating-system source code to the Soviet KGB. In another event, Russian cracker Vladimir Levin,

siphoned $10 million from Citibank and transferred the money to bank accounts around the world [15]. Around the same time the first electronic bulletin board systems (BBSs) sprang up which allowed the phreakers and hackers to gossip trade tips, share stolen computer passwords and credit card numbers, and distribute warez (hacker jargon for pirated software).

With the launch of rich browsers like Netscape Navigator and Microsoft Internet Explorer, during the mid 90s accessing the information on the Web became easy. Hackers now started moving their “how to” information and hacking programs from BBSs to new hacker Web sites. As information and easy-to-use tools become widely available to anyone with Net access, the number of attacks also increased drastically. There were reports by the General Accounting Office that the Defense Department computers sustained 250,000 attacks by hackers in 1995 alone [11].

In the late 1990, Hackers pierced security in Microsoft's Windows operating system to illustrate its weaknesses. Trojan horse virus was released in 1998 by hacking group ‘Cult of the Dead Cow’ which on a machine running Windows 95 or Windows 98, allowed unauthorized remote access of the machine. Spamming attack was also seen during this time. An example of which is the attack on the Federal Bureau of Labor Statistics in 1998, which was inundated for days with hundreds of thousands of fake information requests. The website was brought down that frustrated the economists and investors as they depended on it to retrieve the latest economic data [16]. In addition, Internet portals like Yahoo and AOL were also target of spam attacks. Yahoo was hit by hackers claiming a "logic bomb" will go off in the PCs of Yahoo!'s users on Christmas Day 1997. AOL was a target when AOHell was released which caused the mail box of AOL users to be flooded with multi-megabyte mail bombs and chat rooms to be disrupted with spam messages.

The worms and viruses released in the twenty first century posses a higher impact in terms of financial damage and loss of productivity. An example is the "Love Letter" worm that caught on in May 2000 caused companies $960 million in clean-up costs and $7.7 billion in lost productivity [12]. Nimda and Code Red virus in 2001 ushered new threats that the viruses are capable of spreading across the Internet without any user interaction and then automatically launching further attacks such as denial-of-service (DoS) attack. Microsoft was a target of DNS attack, which took the users to corrupted links and prevented millions of users from reaching Microsoft Web pages for two days. In January 2002, the Slammer worm that spread across the Internet caused short-term Internet outages. In 2004, Mydoom virus caused $43.9 billion in economic damage in 215 countries, according to a report by mi2g Intelligence Unit (mi2g.net), a digital risk firm**.** This virus is considered as the worst virus to ever hit our networks.

Incentives and motivation behind these attacks:

If we examine the early attacks one would see that early hackers were basically programmers who programmed on machines for the sheer joy of it. This curiosity could be interpreted as the essence of hacking in its original sense. Some got involved into this act in an attempt to gain personal fame. Movies such as *WarGames* and Iain Softley's *Hackers* motivated few others as they saw the character of a hacker as a brilliant and romantic guy that breaks the law for noble purposes.

Today's sophisticated attacks posses a greater damage potential. Various claims from hacker groups regarding breaking into Pentagon network to steal military software followed by threats to sell it to terrorists if their demands are not met are on a rise. This is clearly an indication that the face of cyber-criminal activity is changing as we see that the scope and

intention of the attackers has increased beyond control. Hackers are no longer enthusiastic cyber-geeky profiled teenagers but guys with real bad intentions having monetary interests and selfish motives. Today, we see a strong link between the attackers and terrorist organizations who envision cyber-crime as a potential mode to carry out their motive – i.e to spread terror. The below section *"The Attacker – A profile"* has an elaborate discussion on the various profiles and their incentives.

Parallel evolution of Defense:

Preventive measures to defend against the attacks evolved as soon as cyber-criminal activity was discovered and reported. For instance, phone companies started the use of Electronic Switching System (ESS) to counterattack phreaks. ESS made phone phreaking extremely difficult by sending a computer generated artificial ring where the voice is not connected directly to the called party's line unless it's picked up. Since ESS was installed in almost all major cities it made blue boxing harder.

Federal Government also stepped up to stop cyber-criminal activity and enforced a national crackdown on hackers. In the wake of an increasing number of break-ins to government and corporate computers, Congress passed the 'Computer Fraud and Abuse Act' in 1986, which made breaking into computer systems a crime. Also, the 'Comprehensive Crime Control Act' passed in the same year gave Secret Service jurisdiction over credit card and computer fraud (Section Current Law and Policy speaks in detail on this). In addition, the Computer Emergency Response Team was formed by U.S. defense agencies with the mission to investigate the growing volume of attacks on computer networks. Simultaneously, intelligence services such as FBI stepped up and started investigation of hunting down cyber-crackers. In one of the first

arrests of hackers, the FBI busted the Milwaukee-based 414s after members were accused of 60 computer break-ins ranging from Memorial Sloan-Kettering Cancer Center to Los Alamos National Laboratory which helps develop nuclear weapons. [11]

The technology's response to cyber-crime was the invention of IPv6 protocol that supported built-in authentication, integration, confidentiality and access control at the IP layer. Antivirus products from companies like Norton and MacAfee became more prominent for use on home computers. Also realizing series of attacks that exploited security in Windows Operating System and other Microsoft products, Bill Gates outlined his vision for Trustworthy computing [17]. This resulted in more secure products in the current Microsoft releases. There is an effort by software companies to release advisories and patches as soon as vulnerability is discovered in a released product. Security is a key aspect today in the software development lifecycle where security reviews are held, threat modeling is done to do an in depth risk analysis of various potential threats.

What is learnt?

It is safe to proclaim that soon after the first computer networks were built, some people were looking for ways to exploit, thus giving birth to cyber-crime. However, cyber-crime didn't spring up as a full-blown problem overnight. This problem emerged and grew as computing became easier, less expensive, and more easily accessible. As technology advances, vulnerabilities are discovered, and then defenses against those vulnerability evolve. But then new products are released, new security holes are soon discovered and this vicious cycle never ends. With the time tested examples of cyber-attack devastation and the rise of terrorism in the last few years, Cyber-crime has emerged as a serious threat for countries and organizations. The

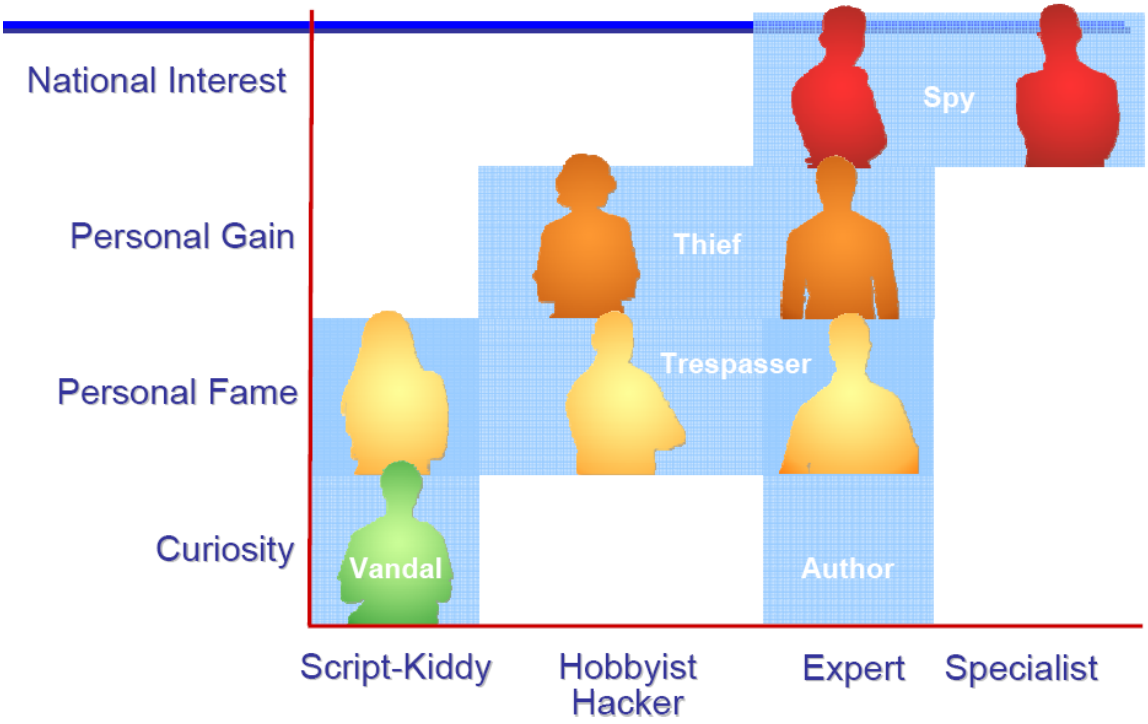
embracement of cyber-crime by terrorist organization has a damage potential beyond imagination.

II. The Attacker – A Profile

No words are stronger than those of the highest ranking federal official involved in the first federal crackdown on hackers in 1990, to indicate the shift of perspective on the hacker profile: "Our experience shows that many computer hacker suspects are no longer misguided teenagers, mischievously playing games with their computers in their bedrooms. Some are now high tech computer operators using computers to engage in unlawful conduct." [19] Earlier accounts of a typical hacker consisted of the simple profile of: white male in his teens, usually intelligent and from an upper middle class family [18]. The simplicity in the original hacker profile could be attributed to many factors including economics that made computers only affordable to a certain class which strongly correlates to racial background. The lack of significant damage potential and perceived financial gain can also be counted among such factors. With all of those factors starting to drastically change around the 1980s and the commoditization of the internet, the hacker profile began to evolve and diversify.

The roots of the hacker profile traces its way back to the phone-phreak descrbed in the History section. Phone-phreaking could be seen as the predecessor of hacking and it existed in a time before computers and modems became flagrantly available. Phreaking is very much alive till this day and could be considered hacking given the blurring of lines between phone and computer, as the former has entered the digital arena and the later being used as a telephony device. Of course with the high degree of connectivity and abundance of bandwidth hackers have more to hack than just phones.

There seems to be several hacker classifications based on intent, damage potential, skill set and so on. People have classified hackers into white-hats and black-hats, referring to good and malicious intent hackers. Other classifications divide hackers into the curious, the meddler and the criminal [18]. A more thorough classification is put forward by David Aucsmith. The Aucsmith classification is a multi-dimension classification based on skill level and motivation. The model is illustrated in the following diagram (courtesy of David Aucsmith)



The skill and motivation ladders start by the 'Vandal' who is relatively inexperienced with little or no significant programming background. Hackers in this category are usually motivated by their curiosity and driven by the desire to achieve personal fame or at least bragging rights among peers. Those hackers are sometimes referred to as script kiddies probably stemming from the fact that they use higher level programming languages like scripts. They mostly rely on information and tools produced by more experienced hackers. Given their age group and relative experience they tend to be less responsible and they are often the class that

releases viruses and worms into the wild. An example of this profile Sven Jaschan, the teenage author of the worm Sasser. Jaschan fits the script-kiddy profile very nicely. He was 17 when he authored the Sasser worm. He is also a relatively inexperienced coder judging by the fact that another worm, Dabber, was built to exploit a vulnerability in Sasser and infect the same hosts.

The model then defines 'Trespassers' who are also driven by the desire for fame but range in their skills all the way to expert. As opposed to releasing worms, trespassers exercise what they know or what they could leverage from more experienced hackers to go to places that they shouldn't. Like the previous profile, financial gain isn't even a factor for them. Even though it might sound irrational to "transcend" without motive but it becomes more understandable considering this profile's mentality as described by Bruce Sterling of the "Hacker Crackdown". According to him trespasser hackers have this sense of being elite, beyond all rules. To them rules are artificial boundaries placed by those with special needs. Hackers make their own rules. This category of hackers also feed on the hacker fuel, bragging, telling the world how great they are. Another motivation is the joy of the ride as described by Kevin Mitnick who was arrested in 1995 after being on the FBI most wanted list for 13 years. According to Mitnick's interview with 60 minutes he felt like "James Bond" when he trespassed into high-defense corporate IT systems. Mitnick's classified his love for hacking as an addiction as he spent 10 to 12 hours daily hacking into systems which also ruined his personal life including his marriage. An addiction would be another way of justifying such an intense desire to trespass for the sake of trespassing.

The third type is the 'Thief' hacker. The thief, as the name implies, is mainly interested in some sort of an illegal gain. Some are intermediate hackers who again rely on tools authored by more experienced hackers or they could be expert hackers authoring their own tools. The

range of crimes is unlimited and the relevant ones to our discussion mentioned through the FBI Cyber Sweep initiative are: “cyber-extortion, economic espionage (Theft of Trade Secrets), Identity Theft and credit card theft”. Due to the money factor, this seems to be the most rampant form of cyber-crime and the most costly to the economy according to Aucsmith. According to the Aucsmith’s analysis this seems to be the fastest growing segment of the hacker population. This is confirmed by the FBI Computer Security Institute annual survey in 2003. The survey outlined the relative annual loss caused by different hacker groups (profiles) on the randomly surveyed companies to be $70.1 million due to theft of proprietary data, and $65.6 million due to denial of service, compared to $27.3 million from viruses. Obscured identity extortionist, “Zilterio”, proudly confessed that companies paid him the “quiet money” sum of $150,000 in an MSNBC email interview. This is a lot of unreported money given the fact that there are probably thousands of “Zilterios” out there. Counter to the norm for this category of hackers “Zilterio” seems to be the vocal type that would email reporters about break-in incidents he committed and agree to online interviews. According to him the publicity is not for personal fame, instead it is a marketing tool. Some hackers in this category also claim that they are on a mission to show the world how bad modern day security is, in addition to making a profit [22].

Finally we come to the ‘Spy’ profile with the highest level of skill set and the biggest impact on national security. Cyber-spies are more determined to achieve their information stealing goal, protected by foreign governments and usually have extensive training. The economic factor can also be present for the spy given the value of information they can retrieve and the abundance of resources under the control of the government they work with. The History section mentions the earliest prosecuted spy hacking case in the US which involved a West-German spy working for the KGB, Markus Hess. Hess was detected in 1986 and

prosecuted in 1990. Spy hackers are usually very sophisticated and use trail covering techniques like relay computers to make it seems like the attack is originating locally and make it harder to trace them [18]. Like in the above example it's typical for the authorities (the US in this case) to take years to successfully track down hackers, capture and prosecute him. Due to the nature of operation in the intelligence business, this profile is the most stealth and hardest to get information about. It's also a profile that has reason and room to flourish according to facts gathered from a CNN analysis report on the post cold war intelligence. The report explains how the internet lends itself to foreign intelligence communities by making it easier to track habits of potential recruits, recruit moles, secure a delivery channel and make it hard to follow their trail. Civil liberties in developed nations, although crucial, make it hard to do counter intelligence [23].

Overall hacking comes in different forms and shapes. As seen form the above discussion motivations for hacking range across different factors like curiosity, love of challenge, ego, economic factors and national interest factors. Despite their differences there seems to be some informal collaboration among different hacker groups, even without explicit intent to collaborate on their part. This happens by information sharing in the hacker underworld through online forums and websites detailing vulnerabilities and demonstrating exploits. Different collaboration avenues are hacker magazines like 2600 and hacker conferences which are outside the scope of this section. One other communality is the impact on society, which extends beyond economic loss and the need to eliminate such disruptive activity.

Doing so is difficult, because cyber-crime covers such a wide range of different actors and methods. Its very nature as non-physical, intangible, impermanent, raises perplexing questions and problems for law, policy, and enforcement. But before any of that, cyber-

criminals must be caught, and here too the digital nature of cyber-crime changes the way the game must be played. The forensics sections shows some of the techniques of identifying cyber-criminals and the laws section discusses laws derived by society to counter such a dangerous and costly activity.

III. Cyber-Forensics and Legal Procedures

The ubiquitous use of computers and other electronic devices is creating a rapidly rising wave of new and stored digital information. About 90% of corporate information currently exists in digital form [1]. Companies generate about 17.5 trillion electronic documents a year. There is also more to this explosive growth than electronic documents. Additional forms of electronic data originate from

- Internet-based electronic commerce, online banking, and stock trading
- Corporate use and storage of phone mail messages and electronic logs
- Personal organizers like the palm pilot and pocket PC that sell about 40 million devices a year.
- Digital cameras
- Corporate use and storage of graphic images, audio and video.

The information risks associated with these data are many. For corporations, the free flow of digital information means that the backdoor is potentially always open to loss. There are several factors as we have seen previously that increase the risk of litigation and loss of confidential corporate data and with this the importance of cyber-forensics grew.

In this information age the physical crimes are somewhat also associated with technology. Some traditional crimes especially those concerning finance and commerce continue to be upgraded technologically. Crimes associated with the theft and manipulation of data is detected daily. A serious and costly terrorist act could come from the internet instead of from a truck bomb. The diary of a serial killer may be recorded on a floppy disk or a hard drive rather than on a piece of paper or a notebook. So as we can see, criminal activity has to some extent converted from a physical dimension in which evidence and investigations are described in tangible terms to a cyber-dimension in which evidence exists only electronically and investigations are conducted online.

It should be also noted that in light of the increased criminal opportunities created by the ever-growing reliance on interconnectedness between network computers, there can be no doubt that experienced and sophisticated computer criminals pose a substantial challenge to law enforcement. There has also been a corresponding increase in the difficulty in catching such criminals. There are a number of reasons why this is so. The anonymity provided by computer communications has long been recognized as one of the major attractions to the would-be computer criminal subjects. This difficulty has been heightened by the use and availability of so-called “anonymizers:” services that repackage electronic mail and thereby diminish the ability to trace it. Furthermore the practice of jumping from comprised network to another comprised network including networks with servers located outside the United States can make tracing down the communication to the initial subject very difficult. This is where the forensics science comes in handy, as we shall see later in this section.

It is also vital to understand that forensic computing, cyber-forensics, or computer forensics, is not solely about computers. It is about rules of evidence, legal processes, and

integrity and continuity of evidence, the clear and concise reporting of factual information to a court of law and the provision of expert opinion concerning the provenance of that evidence [1].

Goals of the forensic investigation

It is important in cyber-forensics to review the reasons why an investigation is needed and the plan of that investigation. It is important to determine the impact and feasibility of conducting an investigation. In some cases, if the cost of the investigations outweighs the benefits, there might not be a reason to conduct the investigation at all.

There are many things (especially in a corporate environment) that might trigger an investigation and some of those are [1]:

- Internet usage exceeds norm
- Using email inappropriately
- Using of internet, e-mail or PC in a non-work-related manner
- Theft of information
- Violation of security policies or procedures
- Intellectual property infractions
- Electronic tampering like fraud, mimicking someone or something, masking or masquerading as someone.
- Network Intrusion which potentially leads to compromising networked computers.

For an investigation to start there should be a justification for a specific complaint or a reason to investigate, and this should be based on rules or a baseline for which a complaint was filed, like violating a standing company policy or procedure. It might also be violating legal statutes, mandatory statutes or regulatory statutes. The investigator must consult these baselines

and rules as appropriate and as part of the investigation to determine how the baseline(s) apply and if there are any documented penalties for such violations. For any of those given violations there are as set of known questions in cyber-forensics that help formalize a plan of investigation. Questions differ based on the reason, and the severity of the offense varies as well.

Once the reasons for an investigation and the baseline have been determined, the impact of the incident must also be determined. By understanding the impact it is determined whether it is feasible to continue on with the investigation. Some incidents regardless of their impact (financial or otherwise) would need to be investigated. Some items that cyber-forensics experts keep in mind when they determine the impact are [1]:

- Benefits to pursuing such an investigation
- Liabilities for not pursuing an investigation
- Obligations to pursue or not to pursue (goodwill toward public, partners and other contracts)
- Resources available (time, people, finances, tools, etc)

It should also be noted that within a company the department with the most experience in conducting an investigation is the internal audit department, although in many cases other departments might be called for assistance like Network Operations, Human Resources, or Legal, and in some cases external consultants might be involved in areas that need expertise. It is a major task during such investigations to properly manage the activities of the investigation while maintaining consistency and integrity of any forensic evidence.

Computer forensic science extracts and produces information. The purpose of the computer examination is to find information related to the case. To support such results, procedures are needed to ensure that only the information exists on the examined media, unaltered. Computer forensics is almost entirely technology and market driven, generally

outside laboratory settings, and the examinations present unique variations in almost every situation.

Steps and Procedures

During an investigation, forensic investigators should be focused on the goal of gathering evidence for prosecution. They should become familiar with federal rules of evidence as well as local and state laws pertaining to the admissibility of evidence and what is required to provide "expert witness" testimony, should that become necessary. Investigators usually work on isolation of equipment, isolation of files, tracking of web sties visited, tracking of log-on durations and times, and tracking of illicit software installation and usage. They then work on correlating all that evidence found. This process is discussed below [1].

Isolation of equipment - Investigators gain approval from management to access the equipment. Once they have the PC or device in their possession they need to preserve the chain of evidence by making sure that neither they nor anyone else is left alone with the equipment. Logs are kept about the whereabouts of and actions taking place on such equipment. It is also important to backup any data under investigation and that the programs used to perform the backup should be independent and have integrity. One good program for such backup is SafeBack [1], which performs a bit-stream backup that helps in making exact partition backups.

Isolation of files - In order to prevent the suspects from tampering with any files, investigators need to disable their user IDs and not delete it. Once IDs are disabled all files they had access to should be copied to a backup media.

Tracking of web sites visited - This happens through reviewing the following items on the isolated equipment (or in other words on the backup of the data on that isolated equipment:

- Cookies, as those take the investigator(s) to the web sites to which the user was visiting.
- Bookmarks where most of the favorite URLs are stored
- History Buffer - these have more information on the timing on which individuals were accessing the websites and could give insights on unapproved or unauthorized web sites.
- Cache from which the investigators can get the last set of instructions or data that was saved to the cache. This requires special programs because it tends to be tricky in many cases.
- Temporary Internet files - This has the advantage over any other items in that it should contain the address of the site, when was it last modified, last accessed, and last checked, and it helps a lot in cases of too much internet access or inappropriate internet access.

Tracking of illicit software installation and use - This is a comparison between the list of programs that currently reside on the PC or device (discovered through inspecting the registry or the files on disk) and the list of what can be on any given PC that follows the corporate policy. These techniques are usually known as System Review. In this the examiner has also to take care of discovering hidden files if any exists.

Intrusion profiling for network intrusion - For network intrusion, it is a bit different than the above. The hacker could be from outside the company. The concept of criminal profiling with a few twists can also be applied for profiling computer / network intrusions. The process of creating the profile involves seeing the intrusion in context, relating the activities to the threat to business functions, and making educated guesses based on probability, experience,

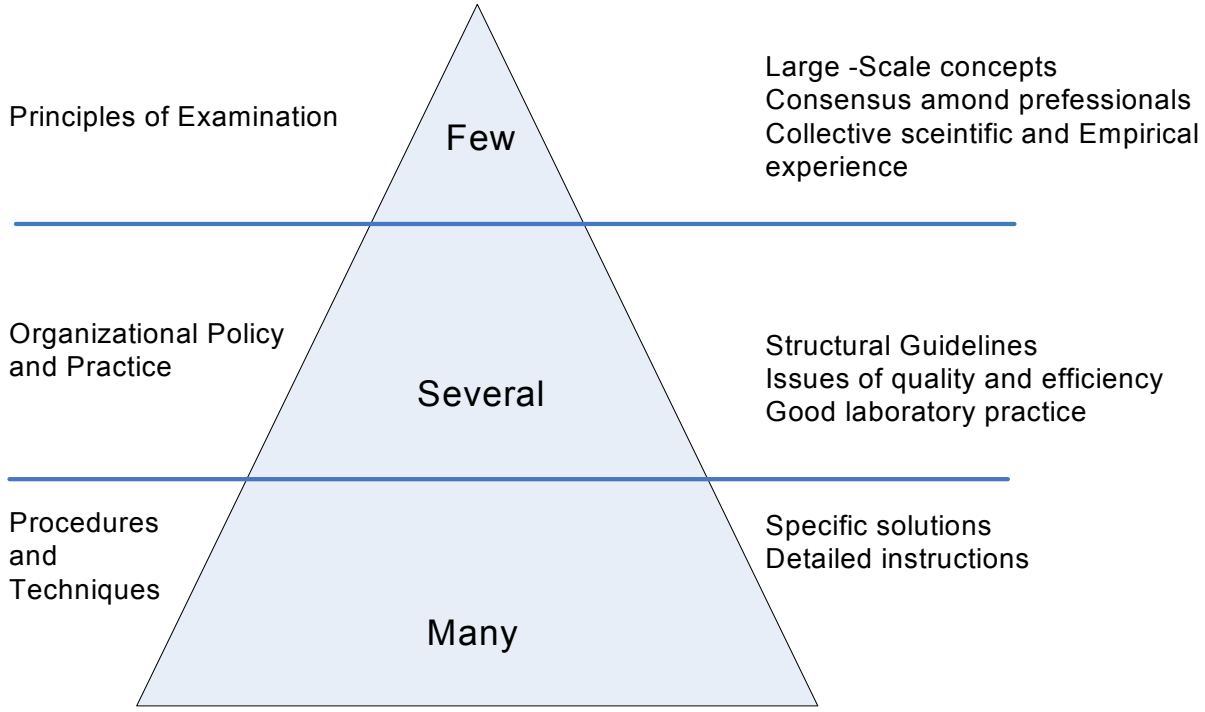
and clues. The profile can assist in tracking the intruder, in identifying future targets, signatures of the attack and possible past intrusion locations, and in assessing the risk or threat of the hacker. The profiling can also reveal possible motives, technical abilities and geographic locations of the hacker.

In order to create a good profile, investigators have to gather information about the time of the intrusion, source of the attack, list of systems penetrated, method of penetration, and list of all files accessed including all written/read and created files. Organizing and compiling such information helps in creating the proper profile that would bring the information together and create an organized picture of who the intruder might be.

Correlating the evidence - Computer evidence as seen from the various listed procedures almost never exists in isolation. It is a product of the data stored, the application used to create and store it, and the computer system that directed these activities. To a lesser extent it is also the product of the software tools used in the laboratory to extract it.

After capturing the file evidence and the data, the examiner can graph an access pattern or list the illegal software or when it was loaded. Next they need to check the access and download dates and times against the time sheets, surveillance and other witness accounts to ensure that the suspect under investigation had the opportunity to engage in unauthorized acts using the equipment in question. Investigators in reviewing such evidence have to show only the facts and nothing else. They can't make any leap in their logic to connect point A to point B as this only show that they lack enough evidence. They also need to be able to adequately explain how the person under review was able to commit the offense, illegal act or unauthorized action and present evidence and proof of how it was done.

In figure (1) below [1], the guidelines for computer forensics evidence are shown:



The figure points out to a three-level hierarchical model consisting of the following:

- An overarching concept of the principles of examination.
- Policies and practices
- Procedures and techniques

Principles of examinations are large-scale concepts that always apply to examination. They represent the collective technical practice and experience of forensic computer examiners. Examples of this in a laboratory may require that the examinations be conducted on copies of the original evidence. Organizational Policy and Practices are structural guidelines that apply to the examination. An example would be creating the required copy and ensuring that it is true and accurate. Procedures and techniques are the software and hardware solutions specific to the given

problem. Examples are Cyclic Redundancy Check and Message Digest, computer algorithms that produce unique mathematical representations of the data which could be calculated for both the original data and the copy and then often compared for identity.

Tools for cyber-forensics

The tools of cyber-forensics can be divided into three different categories: detection tools, protection tools, and analysis tools [1].

Detection tools - These are used to identify risks. They start with network-based tools, one of the most widely used is known as **Nmap**. One of the signature features for this tool is operating system detection through TCP/IP fingerprinting. It also supports dynamic ttl times, parallel scanning and pinging, flexible target and port specification, decoy scanning and output logs to text or machine readable formats. Another tool is **Nessus**, a host-based tool that scans a given host for specific exploits. It is a vulnerability scanner with an excellent GUI front end. **Retina** is another excellent scanner.

In real investigation scenarios a combination of more than one tool is used. For example, to audit a web server for vulnerability, one may first run Nmap, then Nessus, and then follow with a scan from eeye. The above tools are very powerful and actually help exposing lots of vulnerabilities on different systems.

Protection tools - Protection tools mitigate the risk the detection tools identify. They mitigate this risk by increasing either network or host-based countermeasures accounted for in the initial risk formula. Routers, the devices that pass traffic to the correct location, typically form the first line of defense for a network. Firewalls form the second layer of defense in a secured network, and mitigate risk by acting as a sentry for the network and only allowing traffic through that is specifically permitted. Intrusion detection systems (IDSs) function as burglar

alarms for a network by identifying malicious traffic based on signatures. Snort is a good example of such IDS systems. They mitigate risk through increased awareness and knowledge. Proxies act as an insurance policy of sorts by validating that the allowed data is not malicious. Protection tools can be implemented on both the host and the network. Network-based tools tend to be more expensive, more complex, and take longer to implement. However they are vital to the security of the network.

Analysis tools - These tools are used to measure risk. They measure what an incident did and how it was done and what the consequences were. Examples of analysis tools include the Coroners toolkit that runs under NIX and EnCase that runs under Windows.

The importance of a very strong technical ability to use these toolkits cannot be overemphasized. When dealing with cyber-forensics some requirements need to be met. These include a technical awareness through knowledge of the technical implications of actions, an understanding of how data can be modified, cleverness, open-mindedness, deviousness, a high standard of ethics, continuing education and the use of redundant data sources. If one doesn't thoroughly understand or meet the above requirements, the system can be left far worse than when initially compromised from a forensic standpoint. It is like a traffic cop investigating a murder scene (and you get the picture).

I would give an example of one of the tools "EcCase". It provides a familiar Windows Explorer style view. The view displays files without altering them in any way, including free space that contains deleted files. The preview pane is also very helpful when sorting through many files. It has a strong Report view which helps investigators build a case as they proceed. It also allows point-and-click file hashing; an invaluable tool to authenticate files later.

Where does cyber-forensics stand today

After we have looked at the different aspects involved in cyber-forensics analysis and investigations, it might be worthwhile digressing at this stage and looking into real life examples where cyber-forensics had been used and why some of the techniques and procedures mentioned above prove to be reliable and applicable in convicting some criminals.

From the articles referenced in the following links [2] :

- http://www.krollontrack.com/publications/rosenthal.pdf
- http://www.krollontrack.com/publications/kish.pdf
- http://www.boston.com/business/articles/2005/05/11/gillette_workers_may_have_deleted_e_mail/

We would realize that data exist beyond what users expect. Deleting a file for example, does not really mean that it is deleted in most of existing operating systems. It just means that the reference to that file is mangled in some way that makes it invisible to the user. An expert can easily retrieve that file within a certain amount of time. Deleting an e-mail does not mean that it is deleted. On e-mail servers data is backed up every day (and in some cases every few hours) and is maintained for a few months to recover information in case of a catastrophic failure to the system and that means that by proper permission, investigators can get access to this backup media and can retrieve proper e-mails. Also in web sites it turns out to be easy for end users how many references are maintained by the browser for their activity. We have to also make a distinction between the personas involved in cyber-crimes and how well can they cover their trails. In our opinion cyber-forensics has been useful in finding evidence and convicting criminals as witnessed by information available at

http://www.krollontrack.com/publications/SPPP.pdf and other links found of http://www.krollontrack.com/legalresources.

But on the other side, some of the hurdles that might obstruct cyber-forensics would be the expenses incurred in such investigations. Sometimes such expenses are perceived to weigh more than the benefits gained by convicting someone. This might be overcome in the future by having more experts in the field and having more of automated tools. Other obstacles could be the infringement on some privacy laws but that also could be solved by having some updates to some of the existing laws and this could potentially happen in the future once a bigger mass starts realizing the benefits of cyber-forensics.

IV. Current Law and Policy

Provided the technology to catch cyber-criminals exists and is successfully implemented, is our legal system prepared to prosecute? Under which laws' jurisdiction do the various cyber-crimes fall? Knowing, as we do, that policy almost always falls years behind technology, what is the situation currently, and what kinds of steps should be taken to catch up?

The digital nature of cyber-activity renders traditional jurisdictions obsolete. Geographical boundaries mean nothing on the internet and almost all cyber-crime occurs across state lines. This means that although state penal codes like California's do have sections on cyber-crime, most cases fall under federal jurisdiction, specifically under the Computer Fraud and Abuse Act (coded at 18 U.S.C. § 1030). [26] Passed by Congress in 1986, the Act, often referred to as Title 18, is the basic source point for cyber-law, and works as the foundation upon which new legislation is built.

As new technologies, capabilities, and trends appear, the law must be fine-tuned. Rather than combing through the entire United States Code to amend every statute which might be affected by new technologies, legislators must focus careful, substantive amendments on Title 18 and address new problems specifically. For example, in its first incarnation, the law did not even apply to juveniles, who as we now know make up a large percentage of cyber-criminals. [10] Title 18 was amended most significantly in 1996 by the National Information Infrastructure Protection Act of 1996, and as it stands now, holds as its goal the protection of the "confidentiality, integrity, and availability of systems and information." [27] A basic guide from the Department of Justice follows:

	Trespassers	**Authorized Users**
Intentional Damage	*Felony*	*Felony*
Reckless Damage	*Felony*	*No crime*
Negligent Damage	*Misdemeanor*	*No crime*

18 U.S.C. § 1030(a)(5)

As shown, the law is based both on the defendant's authority to access the computer and on his or her criminal intent to cause damage. This means, for example, that if an employee foolishly deletes files from his office computer's hard drive (negligent damage inflicted by an authorized user), he is not punishable by law, as he would be if he were *not* an employee and authorized user of the machine. For a second example, if the employee's teenage daughter hacks

into his office computer as a prank, and *accidentally* deletes the files, she has committed a misdemeanor (negligent damage inflicted by a trespasser).

There is more to cyber-crime prevention than the penal code, however. Various agencies and other policy organizations have in the past two decades participated in different ways in the struggle to design and enforce cyber-law. In 2002, the new Department of Homeland Security recognized the need to consolidate and created the National Cyber Security Division (NCSD) from the Critical Infrastructure Assurance Office, the National Infrastructure Protection Center, the Federal Computer Incident Response Center, and the National Communications System. The NCSD opened in June of 2003 under the supervision of Robert Liscouski and, according to the DHS, works to "identify, analyze and reduce cyber-threats and vulnerabilities; disseminate threat warning information; coordinate incident response; and provide technical assistance in continuity of operations and recovery planning." [28]

For law enforcement, the front lines are held by so-called "CHIP" units, or Computer Hacking and Intellectual Property units. Although the effectiveness of such specialty units is always in question, the Department of Justice claims that in 2003, the first year with all current CHIP units, offices with these units "filed charges against 46 percent more defendants than they had averaged in the four fiscal years prior to the formation of the units." [29]

Of course the current laws and policy are far from perfect. Although doubtful, the possibility of legal loopholes still exists, especially as new technologies appear. Policy is *always* slow, simply because technology evolves faster than Congress passes laws to govern it. Legislation must therefore be carefully crafted to get at generalities and pre-empt silly loopholes. In addition, even if law and policy are entirely up to date, the actual practice of enforcing the

law, implementing the policy, and successfully prosecuting cyber-criminals is very difficult. Although there is still no exact or accurate data on cyber-crime rates, we can say with considerable confidence that as in other types of crime, enforcement capabilities in this area inevitably fall behind criminal capabilities.

This is not to say that cyber-criminals always get away with their crimes. The federal courts do now prosecute cases of cyber-crime, and such prosecutions are currently becoming more and more common. For example, David Smith, perpetrator of the Melissa virus which caused $80 million in damages, was convicted in 2002 and sentenced to twenty months federal imprisonment followed by three years supervised release and ordered to pay a fine of $5,000. [30] In *U.S. v. Jeansonne case*, David Jeansonne of Louisiana received six months in prison and had to pay Microsoft upwards of $27,000 for his Trojan, which interfered with 9-1-1 calls, making the attack what the Justice Department calls a "threat to public health and safety." [31] Still, there is far to go. The first botnet prosecution, *U.S. v. Ancheta*, is only occurring now, as recently as November of 2005. [25]

Of course, it is important to remember that without competent methods of cyber-forensics, any discussion of prosecution is essentially a moot point. That is, the court cannot convict what law enforcement can't *catch*. And the question of forensics also opens up questions of cost-effectiveness and incentives. Are the costs of catching cyber-criminals prohibitive, or do adequate incentives for doing so exist? Are current cyber-forensics methods effective enough to act as a disincentive to criminals?

The future of cyber-law and cyber-security policy remains to be seen, but certain elements are predictable. For one, we can expect (or at least hope for) more specialized law

enforcement like the CHIP units. Just as bomb squads employ explosives experts, cyber-crime units will have to consist of white-hat hackers and computer science professionals. In addition, more coordination between law enforcement and the industry is needed. The recent Sony scandal is just one example of a technology industry giant employing criminal tactics. The industry also needs to be at the table to discuss questions of what should be allowed in terms of grey-hat hacking. Only with cooperation from the industry and academic spheres can the policy world hope to catch up to cyber-criminals.

V. Impacts of in Cyber-Crime and Future Trends

Lunda Wright, a legal researcher specializing in digital forensic law at Rhodes University, has an interesting research finding on a blog posted in October 2005. It states that there has been an increased rate of prosecutions of cyber-criminals. There has been an increased clamping down on cyber-piracy related to the film and music works. There are novel lawsuits and strategies for litigation. There is a greater dependence on the skills of computer forensic experts in corporations and government. Finally, there is an increase in inter-government cooperative efforts.

Organized crime groups are using the Internet for major fraud and theft activities. There are trends indicating organized crime involvement in white-collar crime. As criminals move away from traditional methods, internet-based crime is becoming more prevalent. Internet-based stock fraud has earned criminals millions per year leading to loss to investors, making it a lucrative area for such crime.

Police departments across the nation validate that they have received an increasing number of such crimes reported in recent years. This is in sync with the national trend resulting

from increased computer use, online business, and geeky sophisticated criminals. In the year 2004, cyber-crime generated a higher payback than drug trafficking, and it is set to grow further as the use of technology expands in developing countries.

Scott Borg, director of the U.S. Cyber Consequences Unit, an agency supported by the U.S. Department of Homeland Security, recently indicated that denial-of-service attacks won't be the new wave of future. The worms, viruses are considered 'not quite mature' as compared to the potential of attacks in future.

Potential Economic Impact

As today's consumer has become increasingly dependent on computers, networks, and the information these are used to store and preserve, the risk of being subjected to cyber-crime is high. Some of the surveys conducted in the past have indicated as many as 80% of the companies' surveyed acknowledged financial losses due to computer breaches. The approximate number impacted was $450 million. Almost 10% reported financial fraud [3]. Each week we hear of new attacks on the confidentiality, integrity, and availability of computer systems. This could range from the theft of personally identifiable information to denial of service attacks.

As the economy increases its reliance on the internet, it is exposed to all the threats posed by cyber-criminals. Stocks are traded via internet, bank transactions are performed via internet, purchases are made using credit card via internet. All instances of fraud in such transactions impact the financial state of the affected company and hence the economy.

The disruption of international financial markets could be one of the big impacts and remains a serious concern. The modern economy spans multiple countries and time zones. Such interdependence of the world's economic system means that a disruption in one region of the

world will have ripple effects in other regions. Hence any disruption of these systems would send shock waves outside of the market which is the source of the problem.

Productivity is also at risk. Attacks from worms, viruses, etc take productive time away from the user. Machines could perform more slowly; servers might be in accessible, networks might be jammed, and so on. Such instances of attacks affect the overall productivity of the user and the organization. It has customer service impacts as well, where the external customer sees it as a negative aspect of the organization.

In addition, user concern over potential fraud prevents a substantial cross-section of online shoppers from transacting business. It is clear that a considerable portion of e-commerce revenue is lost due to shopper hesitation, doubt, and worry. These types of consumer trust issues could have serious repercussions and bear going into more detail.

Consumer trust

Since cyber-attackers intrude into others' space and try and break the logic of the page, the end customer visiting the concerned page will be frustrated and discouraged to use the said site on a long term basis. The site in question is termed as the fraudulent, while the criminal masterminding the hidden attack is not recognized as the root cause. This makes the customer lose confidence in the said site and in the internet and its strengths.

According to reports sponsored by the Better Business Bureau Online, over 80% of online shoppers cited security as a primary worry when conducting business over the Internet. About 75% of online shoppers terminate an online transaction when asked for the credit card information. The *perception* that the Internet is rife with credit card fraud and security hazards is growing. This has been a serious problem for e-commerce.

Complicating the matter, consumer perceptions of fraud assess the state to be *worse* than it actually is. Consumer perception can be just as powerful - or damaging - as fact. Hence users' concerns over fraud prevent many online shoppers from transacting business. Concern over the credibility of an e-business in terms of being unsafe or cluttered makes a shopper reluctant to transact business. Even the slightest perception of security risk or amateurish commerce seriously jeopardizes potential business.

Areas Ripe for Exploitation

Modern military of most of the countries depends heavily on advanced computers. Information Warfare, or IW, including network attack, exploitation, and defense, isn't a new national security challenge, but since 9/11 it has gained some additional importance. IW appeals because it can be low-cost, highly effective and provide deniability to the attacker. It can easily spread malware, causing networks to crash and spread misinformation. Since the emphasis is more on non-information warfare, information warfare is definitely ripe for exploration.

Most spammers do not intend to sell. All they want is to obtain the credit card number. Recently this happened to my wife. She received two different emails coming from eBay. These emails asked her to verify the account. They expected her to enter credit card number along with expiration information and the three-digit pin. It even asked her to enter her PIN number for the ATM card. She was taken to a web site which looked like a genuine eBay website with appropriate eBay branding. But such websites are in fact run by fraud rings. Besides the direct loss of credit card and debit card information, such frauds damage popular confidence in the internet and its security, as discussed above. This is a new way of attack that will see new limits in the near future. In the past, hackers were mainly after bragging rights, but professional hackers

are targeting making profits. Hence their determination and the resources they have available are much more.

As more and more firewall hacks are reported there will be an emphasis on having a two-way firewall in every modem. This will secure any inbound attacks and outbound attacks as well. This will certainly be a new avenue that a professional hacker will exploit and find ways to circumvent an apparent security that two-way firewall poses currently.

National Security

The Internet has 90 percent junk and 10 percent good security systems. When intruders find systems that are easy to break into, they simply hack into the system. Terrorists and criminals use information technology to plan and execute their criminal activities. The increase in international interaction and the wide spread usage of IT has facilitated the growth of crime and terrorism. Because of the advanced communication technology people need not be in one country to organize such crime. Hence terrorists and criminals can find security loopholes in the system and can function from unusual locales instead of their country of residence.

Most of such crimes have been originating in developing countries. The widespread corruption in these countries fuel these security hacks. The internet has helped fund such crimes by means of fraudulent bank transactions, money transfer etc. Greater encryption technology is helping these criminal activities.

Future Trends

One of the biggest concerns is what if there is a hack into the critical systems in government, companies, financial institutions etc. This could lead to malware in critical systems

leading to data loss, misuse or even killing the critical systems. Since the communication flow is easy via the internet, the crime organizations might merge and cooperate even more than they are currently.

It is feared that due to enhanced mobility, funds and people could transfer easily. The Internet is increasingly likely to be used for money laundering. As the Internet becomes the medium through which more and more international trade takes place, the opportunities for laundering money through over-invoicing and under-invoicing are likely to grow. Online auctions offer similar opportunities to move money through apparently legitimate purchases, but paying much more than goods are worth. Online gambling also makes it possible to move money especially to offshore financial centers.

Recruitment into crime agencies over internet will be easier than before. Secret messages can be transferred over the internet to a large group of people very easily without being conspicuous.

Because much of the information technology companies are privately owned, the focus would be on making customer happy as opposed to worry about the transnational crime. In addition, legitimate civil liberties could be argued in favor of not monitoring the information technology. All of these things make it more difficult to deal with cyber-crime.

Conclusion

No one could deny that the internet has changed our lives, our culture, and our society in countless ways over the past twenty years. The entire phenomenon is still so new, in fact, that we have yet to discover exactly how we are impacted by it, and in what new ways it will

continue to impact us in the future. We cannot say for certain what new advances the internet will give us, what new art forms, social classes, or subcultures it will engender. Neither can we predict all the dangers which it introduces.

Cyber-crime is necessarily also very new. It is obviously no older than the internet itself. However, it is not any younger either — as soon as there was an internet, there were criminals operating to exploit it. Such is the way with all new technology. We must do our best to keep one step ahead of cyber-crime, in order to best protect ourselves. At the very least, we cannot afford to fall too far behind.

References

[1] Cyber Forensics
A files manual for collecting, examining and preserving evidence of computer crimes
By: Albert J. Marcella and Robert S. Greenfield
ISBN: 0-8493-0955-7

[2] Hacking Exposed – Computer Forensics – Secrets and Solutions
By: Chris Davis, Aaron Philipp and David Cowen
ISBN: 0 – 07- 225675-3

[3] http://usinfo.state.gov/journals/itgic/0801/ijge/gj07.htm

[4] http://www.cwalsh.org/isnd/archives/001270.html

[5] http://www.ci.san-luis-obispo.ca.us/police/cybercrime.asp

[6]
http://computerworld.com/securitytopics/security/cybercrime/story/0,10801,106574,00.html?SKC=cybercrime-106574

[7] Hacker’s biography http://www.rotten.com/library/bio/hackers

[8] Scene of the Cybercrime: Computer Forensics Handbook

By Debra Littlejohn Shinder

http://www.syngress.com/catalog/?pid=2250

[9] Government Technology: Cyber-terrorism in the 21st Century

http://www.governmenttechnologyuk.com/default.asp?id=261

[10] Hacking's History

http://pcworld.about.com/news/Apr102001id45764.htm

[11] Hackers: a St. Petersburg Times series.

http://www.sptimes.com/Hackers

[12] Lessons of 'Love' virus still sinking in

(http://news.com.com/Lessons+of+Love+virus+still+sinking+in/2100-1001_3-257095.html)

[13] TheWHIR's Web Host News

http://www.thewhir.com/marketwatch/

[14] A Short History of Phreaking

http://emmaf.isuisse.com/anarcook/frekhist.htm

[15] Hacking and Hackers

http://www.thocp.net/reference/hacking/hacking.htm

[16] Wahingtonpost.com: The Federal Internet Guide

http://www.washingtonpost.com/wp-srv/national/longterm/fedguide/stories/fig010998.htm

[17] Trustworthy Computing

http://www.microsoft.com/mscorp/execmail/2002/07-18twc.asp

[18] I-Way Robbery: Crime on the Internet (Paperback)
by William C. Boni, Gerald L. Kovacich

[19] http://stuff.mit.edu/hacker/hacker.html

[20] http://www.cbsnews.com/stories/2004/10/20/60II/main650428.shtml

[21]http://www.microsoft.com/smallbusiness/resources/technology/security/hacking_into_the_mind_of_a_hacker.mspx

[22]http://msnbc.msn.com/id/3078571/

[23]http://www.cnn.com/SPECIALS/cold.war/experience/spies/melton.essay/

[24] Chawki, Mohamed. "A Critical Look at the Regulation of Cybercrime." *Computer Crime Research Center*. <http://www.crime-research.org/articles/Critical/>

[25] "Computer Intrusion Cases Index" *Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section.*
<http://www.usdoj.gov/criminal/cybercrime/cccases.html>

[26] Computer Fraud and Abuse Act , 18 U.S.C. § 1030 (1986)

[27] "The National Information Infrastructure Protection Act of 1996: Legislative Analysis." *Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section.*
<http://www.usdoj.gov/criminal/cybercrime/1030_anal.html>

[28] “Ridge Creates New Division to Combat Cyber Threats.” *Department of Homeland Security, Press Room.* <http://www.dhs.gov/dhspublic/display?content=916>

[29] “Computer Hacking and Intellectual Property Unit to be Created at U.S. Attorney's Office in Sacramento.” *Department of Justice, Criminal Division.* <http://www.usdoj.gov/criminal/cybercrime/chips101904.htm>

[30] Leydon, John. “Melissa Virus Author Jailed for 20 Months” *The Register,* May 2002 <http://www.theregister.co.uk/2002/05/01/melissa_virus_author_jailed/>

[31] “Man Sentenced for 911 Trojan.” *Virus Bulletin*, March 2005. **http://www.virusbtn.com/news/virus_news/2005/03_15.xml**

Group 2 Work Breakdown

Section	Title	Lead Author
I	History	Nilkund Aseef
II	The Attacker – A Profile	Ahmed Tolba
III	Cyber-Forensics and Legal Procedures	Khaled Sedky
IV	Current Law and Policy	Pamela Davis
V	Impact of Cyber-Crime and Future Trends	Manish Mittal