Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

An Uneven Playing Field: The Advantages of the Cyber Criminal vs. Law Enforcement-and Some Practical

The computer criminal enjoys several distinct advantages over those security and law enforcement elements arrayed in opposition. This paper offers some observations of the disparities between the criminals manipulating digital data and law enforcement chasing after them; and tenders some suggestions in an effort to even the playing field. This paper does not encompass the issue of international information warfare engaged in by national intelligence agencies, but rather is limited to the threats posed by the free-lance...

Copyright SANS Institute

Author Retains Full Rights

AD

An Uneven Playing Field: The Advantages of the Cyber Criminal vs. Law Enforcement—and Some Practical Suggestions

Introduction

Wherever societal interaction occurs, criminals are sure to follow. The most striking recent example of this is in the realm of what is referred to generally as "computer crimes." As modern society becomes more intertwined with, and dependent upon, the computer through advancements in technology and increasing use of the Internet, the computer criminal is there to turn this beneficial development to his own advantage (the male pronoun is used purposefully as the vast majority of computer criminals have been male). Whether for financial gain or in pursuit of a social or political agenda, or even for the pure malicious challenge of it, computer crimes are committed by a number of perpetrators with varying degrees of ability and connections with each other.

The FBI has reported that such crimes are increasing but that many of these events are not reported. Particularly reluctant are private firms that are concerned with potential negative publicity or concern that proprietary information may be required by investigators. More detailed information may be found at the following URL:

http://www.cnn.com/2002/TECH/internet/04/07/cybercrime.survey/index.html

The computer criminal enjoys several distinct advantages over those security and law enforcement elements arrayed in opposition. This paper offers some observations of the disparities between the criminals manipulating digital data and law enforcement chasing after them; and tenders some suggestions in an effort to even the playing field. This paper does not encompass the issue of international information warfare engaged in by national intelligence agencies, but rather is limited to the threats posed by the free-lance computer criminal generally acting alone or in informal concert with any number of others.

A Brief Overview of Computer Crimes

Computer crimes generally fall into two categories: crimes where the computer itself (or computer network) is the intended victim and use of the computer to commit more traditional crimes. Among the former are denial of service (overloading a system's resources so that it is unable to perform its function), network intrusion, and Internet Protocol (IP) spoofing (inserting a false IP address into a message to disguise the originator).

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Identity fraud is a prime example of the use of the Internet to commit a more traditional crime. Other varieties of fraud also proliferate on the Internet, such as the use of false websites to obtain financial information, as well as, a wide variety of other confidence schemes.

Such activities have a significant negative impact and tend to discourage the full use of tools available on computers that offer the chance for great advancement in knowledge, convenience, and intellectual interaction.

Advantages of the Computer Criminal

1. Networking - A Computer Community Crime Family

Twentieth Century organized crime "families" posed a significant challenge for law enforcement because the hierarchical nature and degree of cooperation presented a more efficient and focused criminal unit. Over time, the law enforcement community was able to meet this threat partly through, in effect, being better organized than the criminal. The degree of cooperation and interaction among computer criminals is similar to that of an organized crime family but on a greater scale, with less personal risk, and without the emphasis on a hierarchy.

The very nature of the Internet allows for unprecedented collaboration and interaction among this particular community of criminals. This degree of interaction nullifies what had been a singular advantage that law enforcement had previously enjoyed over the criminals they were dealing with -- centralized knowledge and superior cooperation.

There are several different forms of cyber criminals.

Although, commonly referred to as "hackers," legitimate computer enthusiasts who enjoy learning programming languages and computers systems (as defined by the Webopedia as referenced in the following URL http://www.webopedia.com/TERM/h/hacker.html resent this association. The term "hacker" is becoming synonymous with individuals who gain unauthorized access to computer systems to steal, alter, or delete data.

"Script kiddies," is defined by Webopedia as referenced in the following URL http://www.webopedia.com/TERM/s/script_kiddie.html as persons who are normally not technologically sophisticated but are able to randomly seek out a specific weakness over the Internet in order to gain root access into a system – exploiting a weakness discovered by someone else.

The term "cyber criminals" will be used for purposes of this discussion – those who use computers and their interconnection to commit crimes. These and others network in underground chat rooms and share their knowledge and exploits with each another. They also use websites to share information such as stolen credit

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

cards, compromised servers, and vulnerabilities in various networks; thereby gaining knowledge needed to further their activities.

The degree of cooperation among the cyber criminal community allows them to take advantage of hardware, operating systems, and software vulnerabilities. Through networking, they download scripts from a variety of hacker websites. They surf the Internet with anonymity and enter unsecured systems at leisure without detection. There is even a tool called "Fragroute," which camouflages hacker programs by manipulating packets of data that travel over the Internet, that bypass intrusion-detection systems and firewalls as reported by the ZDNET. More information relative to the "Fragroute" program and its capabilities can be found at the following URL:

http://zdnet.com.com/2100-1105-887133.html

A group of hackers released a program called Camera/Shy allowing Internet users to hide messages inside photos posted on the Web, again, another tool created to by-pass monitoring software. More information about this freeware promoting free web surfing can be found at URL:

http://www.newsfactor.com/perl/story/18602.html

Cyber criminals conduct reconnaissance on networks and identify vulnerabilities; sharing those with others and then racing to see who can successfully gain access first. They gather and share appropriate tools to exploit the vulnerabilities in order to break into a network or a personal computer. According to computer security expert, Chad Harrington, who regularly surfs Internet Relay Chat (IRC) sites, there are IRC networks with names like "Dalnet "and "Efnet", which are sanctuaries for hackers, similar to an E-Bay site for hackers. More information on these chat sites can be obtained from the following URL:

http://www.cnn.com/2002/TECH/internet/04/10/hackers.chat.rooms/index.html

Those members of the law enforcement community tasked with responding to such cyber crimes are located in a multitude of different agencies at various levels of government. The level of cooperation, although improving somewhat, remains lacking. Improved cooperation is also needed among private sector computer security entities, both with each other and with personnel at relevant government agencies.

By the time security or law enforcement personnel detect a "hack" into an entity's network or into a personal computer, he or she has to start from the beginning and determine the method of the intrusion, the operating system on the computer, learn about the exploits used to conduct the attack, and surreptitiously gather as much digital data as possible relative to the crime.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

At times, law enforcement may be totally dependent upon the expertise of the system administrator of the entity that was breached, or the expertise of a private citizen consultant, because law enforcement lacks the experience or knowledge to respond to the specific type of attack. Unlike the cyber criminal, who utilizes the Internet to gather more information, a limited number of people from law enforcement will be involved in the response to the particular incident, with minimal sharing beyond that core group. Thus, the opportunity to tap into the knowledge and expertise of a wider community is not fully exploited and the lessons learned from a particular event are not fully shared. Hence, delaying the solution of the crime and capture of the perpetrator.

2. Focused Attacks

The computer criminal enjoys the advantage of picking the time, place, and tools of the crime. He can limit his endeavors to his particular specialty. Thus the attacker is often an expert in the means and nature of the crime. The defender, on the other hand, is often a generalist -- one with knowledge of a number of areas but with significant expertise in a limited number (especially relative to computer crimes). If the law enforcement officer has little to no experience with computer crimes, he is at their mercy. Whether he or she has access to the resources necessary to respond to the attack is too often dependent on that individual's own previous efforts in establishing contacts with appropriate expertise, rather than in an agency-wide or inter-agency shared method.

The attack can also be focused in terms of time. Whereas many traditional crimes require a time commitment by the perpetrator -- thereby increasing the exposure and potential for apprehension -- the computer criminal can commit his act in an extremely short period of time with little or no detection by a victim. If he has concealed his identity sufficiently, the computer criminal is free to commit a series of short-term attacks in relative safety.

As reported by Greg Sandoval in the CNET News.com, hackers who attack companies on the Internet are not being caught because law enforcement is having difficulty keeping up the pace with these technologically sophisticated criminals. More information on this never ending battle can be found at URL:

http://news.com.com/2009-1017-912708.html?tag=fd_lede

This particular form of criminal activity is also likely to be committed by an individual acting alone (although knowledge may be shared), depriving law enforcement of such effective tools as confidential informants and undercover operations.

3. Weaknesses of the Defense

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Weaknesses in network security and poor business decisions allow the hackers to proliferate their criminal activities.

One weakness in defending against cyber crime is the inability to secure computers and networks to keep pace with the proliferation of such systems. More people know how to operate computers and set up networks than know how to secure them from attack. Although a growing number of private and governmental entities are improving their security posture, there remains a large amount of vulnerable potential victims.

Another factor is the poor risk assessment decision-making. In this area, risk assessment is the analysis of weighing the risk of the value of a company's assets against the cost of securing them. Too often, a company concludes, after conducting a risk assessment survey, that it is less costly to provide "adequate" security of its network and proprietary database rather than incur the expense associated with proper security. The company decides that in the event of a catastrophic incident, whether it be a natural disaster or a computer intrusion into its network or its database is stolen, the cost of doing business via an insurance or a bonding company is preferable to spending an inordinate amount of money to secure the database with properly trained Information Technology (IT) Personnel well versed in computer security. Subsequently, due to the lack of trained personnel and resources, inadequacies such as misconfiguration of a firewall or of an Intrusion Detection System (IDS), and vulnerabilities in the operating system running on the company's networks may exist. This would provide an opportunity for a cyber criminal to download and steal the company's database containing customer credit card information. Management unfamiliar with computer security may believe that having a firewall is sufficient because they don't understand the full impact of a security breach, which would directly affect the organization's reputation and financial status.

In addition to lax security, many private and public entities do not have an adequate computer incident response procedure. Because most such entities do not have a Computer Incident Response Team (CIRT) to react to a computer incident, concerns such as crime scene security and evidence preservation are often minimal or absent altogether. Evidence may be mishandled, allowing it to be altered or deleted. At times, evidence is nonexistent because IT personnel did not have logs turned on to record the activity on the network. In most digital crimes, log data is the primary evidence that a crime has occurred. If the business did not have a set policy or procedure to have the logs "turned on," there is no evidence there was a crime. Even if the logs were "turned on," a talented hacker has the ability to erase his tracks. Additionally, if the company does not maintain updated back up tapes, other pertinent digital evidence may be lost. For law enforcement, trace evidence in the log files are crucial in obtaining search warrants and subpoenas required in tracking down the hacker. Failure to preserve evidence of the crime would preclude prosecution, even if the elusive cyber criminal is eventually identified.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The nature of marketing in the national economy and doing business on the Internet can result in the exposure of a customer's personal information to cyber crime. In order to obtain business, a company engaging in Internet-related activity must convince potential customers that their website or transaction conducted on its website is secure and will not be compromised. Too often, the sense of security obtained through successful marketing is false. On a company Electronic-commerce website, a customer provides sensitive personal data and credit card information, believing his information is secure. The information may appear that it is being transferred via a Secure Socket Layer (SSL).

Webopedia defines SSL as a protocol developed by Netscape to encrypt and transmit documents over the Internet. Webopedia's SSL definition can be found at URL:

http://www.webopedia.com/TERM/S/SSL.html

However, if the data is stored on the company's server unencrypted, the data is not secure. If the server's operating system is not "patched" properly with the most updated vulnerability patches or if the customer's data is residing on the company's server without encryption and its data is being stored in plain text, a hacker can gain access to it and manipulate the data to commit theft and identity theft. Additionally, the hacker can also commit extortion against the company by removing the company's database and demanding payment in exchange for returning the database to the company, thereby threatening the public image of the company and its financial position.

Management's lack of knowledge concerning computer security and appreciation of the IT staff can result in failure to accurately recognize the risk posed by cyber criminals. In many private entities and governmental offices, senior management tend to be more mature individuals who did not come of age with the computer. In an atmosphere of budgetary constraints, such management may be tempted to cut funding and staffing for IT departments. Moreover, budgetary concerns may preclude the purchase of up-to-date hardware and software -- leading to increased vulnerability. All too often, a catastrophic event, such as compromise of a customer's personal and financial information or well publicized vandalism of a website, is the wake-up call needed for an appropriate response -- but by then, it is too late and the response becomes more damage control.

4. Jurisdictional Advantages

The nature of the medium in which the crime is committed heavily favors the cyber criminal. Cyber criminals have no boundaries. The actions taken in the security of their residence can have an effect hundreds or thousands of miles away, across interstate and international boundaries. Most law enforcement agencies have geographical limits that comprise their jurisdiction. Exceeding such limits requires

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

coordination with other agencies who may not share the same view regarding the seriousness of the crime or may, for any number of other reasons, not feel an urgency to cooperate. Additional obstructions are present if the cyber criminal is located in a country that does not enjoy good relations with the United States. To expect cooperation from law enforcement entities in such countries is optimistic, at best.

5. Prosecutorial process favors Cyber Criminals

Once the cyber criminal is identified, and assuming the evidence has been properly obtained and preserved, the next step in the process all too often favors the cyber criminal. That is, in convincing a typically overburdened prosecutorial office to actually commit the resources necessary to see the matter through to conviction. Most prosecutors, subjected to limited resources and political concerns, devote most of their efforts to those crimes perceived by the public as posing the greatest danger. These usually include crimes of violence and drug related offenses. Cyber crimes are viewed more as the so called white-collar type of crime and usually not given high priority by most prosecutors.

Those cases that do result in a successful prosecution are then subject to a punishment decision by a judge who generally is accustomed to dealing with more violent crimes. Again, the cyber criminal is treated as a white-collar type criminal and given a lenient sentence. The deterrent effect on others is minimal.

Moreover, current federal and state laws are somewhat antiquated as applied to the various types of high technology and cyber crimes being committed. Cyber criminals are mindful and scornful of such laws. In fact, at the renowned hacker conference called DEFCON, which has gathered at Las Vegas, NV for the past several years, a variety of hacker enthusiasts conduct seminars on averting state and federal statutes relative to computer crimes. They discuss ways to avoid being criminally prosecuted by limiting the total dollar damage to a network and also stress that moreover juveniles, are basically exempt from federal prosecution. Judges unfamiliar with computer technology and unable to understand the facts of the computer crime committed fail to appreciate the impact of the crime and provide the proper punishment.

6. Humans want to Trust other Humans

Humans are very trusting and have an inert emotion to help others. Hackers take advantage of this by conducting what is called “social engineering” to deceive people into surrendering passwords and sensitive data about their network unknowingly allowing cyber criminals to use the information to break into computer networks. Recently, AT&T was progressive enough to warn its employees of being socially engineered, as reported by an ZDNet at URL:

http://zdnet.com.com/2110-1105-943604.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Suggestions to Even the Playing Field

1. Education for Law Enforcement, Security Personnel, and Management

Current efforts at training law enforcement personnel to investigate cyber crimes, and the coordination among various law enforcement entities, need to be vigorously improved and expanded. Agency budgeting priorities need to be adjusted to allow for the devotion of adequate resources in this area. If information technology is to play a major part in our future, as it must, then an adequate foundation for a law enforcement posture must be laid.
There are some positive steps being taken in this area. For example, the University of Texas at Dallas joined forces with the Greater Dallas Crime Commission, law enforcement and businesses to create the "Digital Forensics and Security Institute" to combat cyber crimes. The institute will offer a cyber security degree program that includes classes in digital forensics encryption and wireless security. Additionally, courses will be offered to business managers and law enforcement officers who can learn about basic computer architecture, secure access to databases, and recovering information from computers without compromising evidence. More information relative to this collaborative effort can be found at the following URL:

http://www.utdallas.edu/utdgeneral/news/cybercrime.html

In general, management, whether in government or private sector, has to be educated on the importance of computer security. Law enforcement management needs to increase the number of specially trained personnel and invest in the procurement of a variety of hardware and software to combat and resolve computer crimes. In the private sector, managers need to realize that computer security and information technology are relevant to their company's financial well-being. Managers need to assess the proper risks the company is taking if certain computer security procedures are not adhered to and how that could affect their company's "bottom line," hence affecting profits and causing stock prices to go down. There are non-technical courses offered by a variety of computer security training facilities, specifically designed for these managers.

A variety of computer security training courses are offered for System Administrators, and Computer Security and Information Technology Personnel. A number of certifications are specific to law enforcement and management personnel. Many of the law enforcement specific courses are restricted due to the methodologies discussed in tracking the variety of criminals in cyber space. The following organizations offer an array of computer training and security courses.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Organization	URL	Training
SANS Institute	http://www.sans.org/newlook/	System Administration, Networking and Security
Foundstone	http://www.foundstone.com	Audit, assess and secure networks, hosts and applications
CSI Information Security Seminars	http://www.gocsi.com/infosec/wkshop.html	Seminars in Internet Security, Intrusion Management, Intro to Computer Security, Windows 2000, Network Security, & Forensics
SYTEX, Inc	http://www.sytexinc.com/services/training.html	Networks, Computer Intrusions, NT Network Assessment, Computer and World Wide Web Security geared towards Law Enforcement
Federal Law Enforcement Training Center	http://www.ustreas.gov/enforcement/enforc01.html	Law Enforcement courses in Computer Crime Prosecution, Computer Evidence Analysis, Seized Computer Evidence Recovery Specialist, Telecommunications Fraud, & Criminal Investigations in an Automated Environment
National White Collar Crime Center	http://www.brianbrowning.com/nw3ctraining/default.htm	Basic Data Recovery and Analysis & Advanced Data Recovery and Analysis
Blackhat	http://www.blackhat.com/main.html	Seminars on Windows Security, Computer Forensics, Web Applications, Securing UNIX, Hacking, Software Vulnerabilities,
MIS Training Institute	http://www.misti.com/index.asp?region=1	Audit and information security training

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

AntiOnline IT Career Center	http://careers.antionline.com/candidates/resourcepages_technicaltrainingresources/	Information Technology, Internet, Programming, & Database, MCSE, MCSD, MOUS, CCNE, CCNA, MCP CNE, CNE, CLP, A++, UNIX, C/C++, Java, web t technology certifications

2. Update Laws and Train Legal Professionals Specific to Computer Crimes

There have been some efforts to designate various Assistant United States Attorneys as specialists in computer crime prosecution. This trend should be energetically pursued and expanded to include all prosecutorial agencies. It would also be beneficial to identify those judges who are knowledgeable in this area to sit on such cases.

The best efforts of law enforcement and prosecutors will be thwarted without significant changes and updates to current laws relative to cyber crimes. An encouraging sign is the recent consideration by the U.S. House of Representatives of a new cyber crime bill, under which greater surveillance and penalties are provided. More information on this bill can be found at the following URL:

http://www.ananova.com/news/story/sm_630003.html

Although this was primarily in response to cyber terrorism, the tools that would be available will be useful against the typical cyber criminal. Factors such as the cyber criminal's intent and whether sensitive government computers were targeted would play into the punishment. If human lives were knowingly or recklessly put at risk, a sentence of life imprisonment would be available. Internet Service Providers (ISP) would be able to monitor use activity on a more active basis and be immune from privacy-based lawsuits.

Cyber criminals should be punished based on the number of victims, not the number of acts committed. Thus, if the actions of a cyber criminal affect thousands of people, he should be punished accordingly. State laws should be updated and changed to reflect the havoc the cyber criminal creates.

3. Incentives for Law Enforcement Personnel and Security Personnel

Besides the training of law enforcement and prosecutorial personnel discussed above, as a practical matter it is necessary to ensure that those trained individuals remain with the organization. All too often, a governmental agency will provide training to make an individual computer literate, only to lose that person to the private sector. Governmental agencies need to realize such specially trained

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

personnel are a resource worth preserving, either through clearly defined career paths or monetary incentives competitive to the private sector.

4. Taking Advantage of On-Line Resources

Unlike the cyber criminal who learns how to commit cyber attacks from a variety of resources, law enforcement may not have the luxury of the same type of support. By taking advantage of On-Line Resources available on the Internet, an investigator pursuing a computer crime can find resources to successfully help him catch the perpetrator of the crime. The following are some of the websites that may be helpful to the computer crimes investigator and can be book-marked into the investigator's browser allowing easier access when research is needed.

Website	URL	Contents
Computer Crime & Intellectual Property Section (CCIPS) of the Criminal Division of the US Department of Justice	http://www.cybercrime.gov	Computer crime policy, guidance, laws, recent case laws, & Computer search and seizure manual
Find law	http://www.findlaw.com	Federal and state computer crimes statutes & cases
Foundstone	http://www.foundstone.com/knowledge/free_tools.html	Free assessment, forensic, intrusion detection, and scanning tools
DEFCON	http://www.defcon.org/book-list.html	Hackers recommend books on computer security, cyber issues, computer references, & computer underground
National Institute of Standards and Technology Computer Security Resource Center (CSRC)	http://csrc.nist.gov/	Computer Security Resources & Cryptographic standards and applications.
Security Focus	http://www.securityfocus.net	Vulnerability database, computer security issues

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Department of Justice Internet Fraud	http://www.internetfraud.usdoj.gov/#What%20Is%20Internet%20Fraud	Information on Internet Fraud

5. Cooperation between Federal, State, and Local Law Enforcement Personnel

Bureaucratic constraints and concerns over jurisdictional "turf" need to be overcome to allow for complete cooperation. Across the country, numerous High-Technology Task Forces have been created and have been very successful in combating cyber crimes. Turf issues have to be put aside and all components of the law enforcement community have to join and share hardware and software resources to combat cyber crimes. Task forces crossing Federal, State, and Local boundaries can pool their budgets and share resources to successfully work with one another.

6. Cooperation between Law Enforcement and Private Sector

Although, Law Enforcement is slowly catching up in combating computer crimes, it is crucial to maintain partnerships with the private sector to gain confidence and trust amongst the two. By doing so, traditional barriers of non-repudiation will be broken and they can help one another in capturing the criminal in cyberspace. It must be recognized that the private entity IT security personnel play a vital role in controlling cyber crime. Accordingly, efforts must be made to reach out to such individuals to ensure they are adequately trained and aware of proper response techniques.

Two organizations that promote sharing of information and trust among law enforcement and the private sector include the Infragard and the High Tech Crime Investigation Association (HTCIA).

Infragard is led by the FBI and is a cooperative relationship between the U.S. Government and an association of businesses, academic institutions, and state and local law enforcement agencies dedicated to increasing the security of the critical infrastructures of the United States. Detailed information relative to the Infragard can be found at URL:

http://www.infragard.net

A growing organization, HTCIA promotes voluntary exchange of data among computer crimes investigators and senior security personnel. Information relative to HTCIA can be found at the following URL:

http://www.htcia.org

7. Promoting Public Awareness

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The general public and private businesses have to be aware of the increasing cyber crime and must be educated in reporting cyber crime, just as they would a general crime such as an assault, burglary, theft, arson, and others. It would be helpful if the cyber crimes could be reported to one specific organization or a telephone number locally which would be interconnected to all other local, state, and federal law enforcement agencies, thus allowing the computer crime to be pursued by the appropriate law enforcement entity. Since cyber crimes normally cross various jurisdictional boundaries, this sharing of data in one computer system would allow all law enforcement agencies to reference the crimes and be able to cross-reference the information to assist one another in solving crimes that exceed jurisdictional boundaries.

References

CNN.com-FBI: Cybercrime rising Yet fewer companies reporting incidents
http://www.cnn.com/2002/TECH/internet/04/07/cybercrime.survey/index.html

Organized, well-financed criminals stay a step ahead of the law
http://news.com.com/2009-1017-912708.html?tag=fd_lede

Webopedia definitions
http://www.webopedia.com/TERM/h/hacker.html
http://www.webopedia.com/TERM/s/script_kiddie.html
http://www.webopedia.com/TERM/S/SSL.html

New tool camouflages hacker programs
http://zdnet.com.com/2100-1105-887133.html

Free Hacker Software Called Human Rights Weapon
http://www.newsfactor.com/perl/story/18602.html

AT&T warns workers not to be duped by hackers
http://zdnet.com.com/2110-1105-943604.html

Chat rooms a haven for hackers-Anonymously stealing, trading personal information
http://www.cnn.com/2002/TECH/internet/04/10/hackers.chat.rooms/index.html

UT Dallas to Establish Digital Forensics and Security Institute
http://www.utdallas.edu/utdgeneral/news/cybercrime.html

U S Cyber crime bill passed by House of Representatives
http://www.ananova.com/news/story/sm_630003.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice
http://www.cybercrime.gov

Find Law
http://www.findlaw.com

SANS Institute
http://www.sans.org/newlook/home.php

Foundstone
http://www.foundstone.com

SYTEX, Inc
http://www.sytexinc.com/services/courses.html

Federal Law Enforcement Training Center
http://www.ustreas.gov/enforcement/enforc01.html

National White Collar Crime Center
http://www.brianbrowning.com/nw3ctraining/schedules/schedules_home.htm

Blackhat
http://www.blackhat.com/main.html

DEFCON
http://www.defcon.org/book-list.html

National Institute of Standards and Technology
http://csrc.nist.gov

MIS Training Institute
http://www.misti.com/index.asp?region=1

AntiOnline.com "Hackers Know the Weaknesses in Your System. Shouldn't You?"
http://www.antionline.com

Department of Justice Internet Fraud
http://www.internetfraud.usdoj.gov/#What%20Is%20Internet%20Fraud

Security Focus
http://www.securityfocus.net

© SANS Institute 2002, Author retains full rights.

CSI Information Security Seminars
http://www.gocsi.com/infosec

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**