Global Information Assurance Certification Paper

CYBERCRIME: Truth and Consequences

GSEC Practical v.1.4

Submitted by:

Sharon S. Reed

May 13, 2002

CYBERCRIME: Truth and Consequences

Introduction

We are a nation with a competitive spirit and a desire to succeed and lead. This is very evident in our high-tech society. Technology has propelled us into uncharted territory and provides us with amazing advancements and conveniences we have become acutely dependent upon. The global network was designed to create a borderless means of communication and information sharing and, at the same time, has seamlessly interconnected the basic framework of our society: social, economic, and political. The same networking advancements that have made our nation strong are the same elements that make us vulnerable. As technology grows exponentially so do the risks involved in protecting vital information and critical infrastructures. Computers have become extremely powerful. They can remotely transfer funds, manage weapon systems, control power grids, monitor air traffic, etc with little effort. Neglecting to implement appropriate defensive measures within your own organization can make you vulnerable to attack, and that impact can have a devastating ripple effect.

The goal of this paper is to promote computer security awareness and ultimately provoke you to re-address your own security practices on your systems at work and at home. Positive changes are being made, but so much more must be done to correct years of complacency. A vigilant eye and clear understanding of the threat can mean the difference between victor and victim.

Executive Summary

The United States, or the world for that matter, do not fully comprehend the magnitude of the crimes being perpetrated by unauthorized individuals on business and government computer systems. Cybercrimes are severely underreported and don't provide us with an accurate assessment of the financial losses and the profound implications of stolen intellectual property, sensitive classified information, and/or sensitive personal information. To put this in more tangible terms, the FBI and San Francisco's Computer Security Institute (CSI) conducted a recent survey of 503 computer security specialists and reported that the numbers of computer penetrations and the economic losses associated with them are soaring. 223 respondents in the survey reported financial losses of $455 million, up from the previous year.[1] Losses this year have continued to spike upwards, but because so few companies report their losses or the fact they've been "hacked" into, these statistics only offer us a 'best guess' as to what is actually taking place. These results represent a small segment of the population and true estimates of the entire population would undoubtedly be staggering.

The thrust to automate sectors such as health, government, education and banking has caused us to become easy targets for computer criminals. This is no longer an individual or isolated problem. Corporations, governments, and countries need to unite and join efforts in protecting the stability of world economics and the safety of our society against potential

catastrophic attacks. It is important to emphasize that everyone is at risk and has an obligation to mitigate and report computer crime so effective defenses can be put in place.

State of Security

Computer crimes include the illegal use of, or the unauthorized entry into a computer system, to tamper, interfere, damage or manipulate the system or data. [2] It is easy to say the problem is overwhelming, but supporting statistical information presents a clear assessment of the situation. Provided are a few convincing statistics that emphasize the importance of security and should provoke a call to action.

- A new Computer Emergency Response Team (CERT) survey shows the alarming rate at which reported security incidents are escalating. By the fourth quarter of 2002, reported incidents are expected to substantially exceed 100,000, a rate that is more than doubling each year. [3]

CERT/CC Statistics 1988-2002

Number of incidents reported

1988-1989

Year	1988	1989
Incidents	6	132

1990-1999

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999*
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000-2002

Year	2000	2001	Q1,2002
Incidents	21,756	52,658	26,829

http://www.cert.org/stats/cert_stats.html

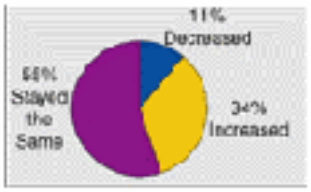
Figure 1 **Total incidents reported (1988-Q1,2002): 127,198**

- According to the American Society for Industrial Security, since the mid-1990's, American businesses have been losing $250 billion a year from intellectual property theft.[4]

- Industry analysts estimate 70% to 90% of all attacks on corporate networks occur internally. To compound matters, insider breaches are a hundred times more costly than attacks from outside the enterprise. [5]

- Pilot Network Services, an Alameda, California firm that makes firewall software, reported in April of 2001 that the company discovered 95 million attempted entries had been detected by computers using Pilot's protective program—a 220% increase over the number detected the previous month. [6]

• Based on the September 11, 2001 terrorist attacks in Manhattan and at the Pentagon, Computer Economics examined several factors and interviewed information technology and communications workers to analyze the economic impact on these services. Compiled information shows the costs of restoring IT and communications capabilities could cost as much as $15.8 billion. [7]



IT Budget for Security Spending Since 9-11

http://www.computereconomics.com/article.cfm?id=538

• *Figure 2* reflects the incredible financial losses from e-mail viruses.[7]

The Computer Economics Security Review 2002

Analysis By Incident

Year	Code Name	Worldwide Economic Impact ($ U.S.)	Cyber Attack Index
2001	Nimda	$635 Million	0.73
2001	Code Red(s)	$2.62 Billion	2.99
2001	SirCam	$1.15 Billion	1.31
2000	Love Bug	$8.75 Billion	10.00
1999	Melissa	$1.10 Billion	1.26
1999	Explorer	$1.02 Billion	1.17

http://www.computereconomics.com/article.cfm?id=356 *April 2, 2002*

Figure 2

The examples above show current losses are tremendous and only expected to grow. The actions of cybercriminals can no longer be underestimated. They are the high-tech burglars of today that sneak across network connections and secretly steal, vandalize, and destroy information at a phenomenal cost to the economy.

Who are the Offenders?

Hackers, crackers, script kiddies, and employees are commonly the offenders who pose a threat to your computer security. Understanding their differences and motivation can provide important insight and offer a different security perspective to your own situation. Motivation varies from individual challenge, recognition, revenge, defiance, financial gain, political reasons, altruistic purposes or causes, to gain a competitive edge or the more extreme groups who advocate terrorism and chaos. These groups understand that what they are doing is illegal and use many different tactics and techniques to infiltrate your system.

*A **"Hacker's"*** primary motivation is knowledge. Hackers do not want the publicity crackers prefer. Rather, it is important to remain undetected as they explore restricted computer systems and take the system's programming beyond its known limitations. The term ***"Cracker"*** was created by hackers who wanted to distance themselves from the practices of crackers. Crackers do not share the same technical prowess of hackers when

breaking into a system. Instead they use persistence, determination, and widely available hacking tools and tips to allow them to exploit well-known vulnerabilities in targeted systems. Their motivation can include the thrill of the challenge, profit, or because of some strong belief or cause. ***"Script Kiddies"*** *are* normally not technologically sophisticated. They randomly seek out a specific known weakness over the Internet in order to gain root access to a system without exactly understanding what it is s/he is exploiting. A script kiddie is not looking to target specific information or a specific company but rather uses their knowledge of a vulnerability to scan the entire Internet for a victim that possesses that vulnerability. Most often they are the ones to get caught because of their inexperience. ***"Employees"***, whether disgruntled or unwitting, are responsible for huge losses associated with fraud, theft, unauthorized access, data corruption, and misuse of equipment, software and communication lines. Approximately 80% of computer crimes originate inside the network. Preventative measures focus primarily on larger external threats, all the while 'smaller' internal threats can easily be overlooked. [8]

Preventative Measures

There is an abundance of hardware and software tools available to protect and monitor your computer systems. Information technology vendors promoting their security solution have galvanized their presence in an exploding high-tech market. Aggressive competition among these players stimulates the rapid advancement of technology and stretches its limitations. Applying these technologies is paramount to a secure system, but many tend to overlook the more obscure practices that are equally as important as 'shrink-wrapped' products. Each of the points listed should be the foundation on which all other security measures are applied, but how many of these practices fall short or do not exist at all?

- Companies must reevaluate their organizational priorities. There was a time when "security" was not a high priority to the overall mission. A negligible budget was set aside to address routine security concerns. These changing times have made security and survivability codependent. Budgets should address training, qualified personnel, and the latest hardware and software tools. Careful cost and risk analysis can determine the level of security and the price tag each system will require.

- Ongoing technical training is essential. It is a highly effective means for IT professionals to stay current with the latest technology and to use that knowledge to ward off criminal activity. Training allows IT professionals to effectively install, configure, and achieve the highest level of functionality when using the latest hardware and software detection tools.

- Take a close look at your security policies or the lack thereof. Are they current? Insure they cover critical areas such as physical security, personnel security, configuration management, encryption, virus protection, passwords, security awareness training, incident response, backup/recovery options, remote access, identification and authentication, information handling, and so on. Policies should address all aspects of your day-to-day business activities and should be enforced at all levels.

• Security awareness training for all employees should be common practice. Losses stemming from social engineering, a non-technical form of intrusion, are all too common. Training and sound implementation of policies provides a security-conscious organization with clear guidelines. Minimizing unintentional disclosure of information or deviations from normal security procedures is the primary objective.

• Technology is constantly evolving and becoming more powerful. This evolution offers improved hardware and software tools that provide a significant layer of defense and can mean the difference between successful infiltration and a failed attempt. Defense in depth means there is no such thing as one solution. Firewalls, intrusion detection systems, segmented networks, etc. all have their place and careful analysis of your company and its systems can help to determine what information is valuable and warrants the most protection.

• Give careful concern when hiring employees to safeguard your company's most valuable assets. IT has historically received less than adequate manpower attention. In order to overcome this challenge, we must consider options outside standard human resource practices. To attract and retain foreword-thinking individuals with the foresight and skill to anticipate and proactively address problems associated with system security, incentives must be enticing and substantial. The hiring criteria for key strategic positions must clearly be defined. Once defined, it is possible to take advantage of the specific strengths and abilities of current employees and realign your IT structure. A probationary period should be a condition of employment with incentives for proven performance. Target new employees who are capable of effectively resolving identified weaknesses within the organization. Finally, review salary and benefits annually to make sure they remain attractive and competitive. The bottom line is *mediocre employees produce mediocre results*.

• Hire an outside auditor to come in to conduct internal and external penetration tests on your systems. This provides a level on insurance and implements a procedure of "checks and balances" on your system and the employees who support it. They can analyze the system's security posture and provide an impartial report.

• Know your computer network. Maintain a current and accurate blueprint of your network system and all its connections. Be aware of potential backdoors and be vigilant in knowing what is happening on your network.

• Report any unusual activity. Refer to company incident reporting policy to document and submit incident reports. Not informing the proper personnel is a huge disservice to your organization. Incident reporting can yield additional funding to improve your company's security posture. If management does not know of security issues, how can they support additional protection measures?

• Monitor, monitor, monitor!!! Security tools are only as good as the data gathered from them. Businesses have downsized due to economic conditions and the new attitude is to

"do more with less". It is easy to get caught up with the everyday tasks and overlook the less visible, but fundamentally significant functions of security. Continue to monitor and faithfully review security logs.

- Join professional computer groups and network with experienced peers. There is a wealth of knowledge available and many people are eager to share their technical expertise. Take advantage of these resources.

- Read the latest computer technology magazines and on-line articles. Join on-line newsgroups to stay informed of timely information such as patches, alerts, viruses, and vulnerabilities.

Obstacles

It is virtually impossible to create an IT solution that will blanket the entire problem of network security and cybercrime. The problem is vast, complex and riddled with obstacles. Despite the overwhelming challenge, governments, federal, state, and local law enforcement agencies, and IT vendors are beginning to move this mountain one stone at a time.

From a legal standpoint, law enforcement is not prepared to deal with the emergence of this type of crime. Computer-based crime is costly and law enforcement does not have all the necessary resources such as personnel, technology, equipment, funding, or legal direction to investigate and effectively prosecute them. Alan Benitez, a special agent with the California Department of Justice who specializes in computer crime investigations said, "Crimes against people takes priority. When a company comes in and says they lost money and need our help, they are probably real low on the list" compared with the response to a violent crime victim. [9] On a more international level, Rajesh Sreenivasan, a Singapore lawyer states, "The physical problems that arise from dealing with computer criminals are the difficulty in tracing, prosecuting, and reaching a desired verdict. If a crime crosses borders, it may be almost impossible to secure extradition or decide which country deserves ultimate jurisdictional power over a given case. As such, laws concerning computer crimes need to be made extra-territorial as well as specific. As the present legislation is inadequate for dealing with computer crimes, laws that allow for practical enforcement are greatly needed. The law must take into consideration the admissibility of digital evidence that may be transient." [10] These viewpoints are not shocking, however they should serve as a wakeup call to the legal system. The problem is clear and the weaknesses are well defined. Aggressive changes around the world are well overdue.

Another obstacle preventing swift change is the lack of hard statistics due to weak reporting. There are many agencies that publish statistical information on individual studies. Unfortunately, there is no single entity overseeing the management and security of the Internet and there is no standard on how to organize statistical information. Therefore, in order to form our conclusions, we must rely on results from literally thousands of individual studies conducted on small segments of the population. The global response and the level of attention are based on those approximations. Hard statistics help identify the

totality of the problem allowing for a well-measured and precise course of action to combat it. Undoubtedly, if losses were accurately quantified, it would provoke an abrupt response that would equal the severity of the problem.

"There is much more illegal and unauthorized activity going on in cyberspace than corporations admit to their clients, stockholders and business partners, or report to law enforcement." *Patrice Rapalus, Director of the Computer Security Institute*

An FBI survey conducted in 2002 revealed 90% of the respondents detected security breaches and only 34% reported those attacks to authorities. [11] Why are so many computer crimes underreported?

- System and network administrators are not aware their systems have been compromised. The reasons can range from lack of detection tools, inadequate manpower due to budgetary constraints, or just poor security practices. Regardless of the reason, this can be very costly.

- Another reason for not reporting computer attacks is to prevent bad publicity. Keeping the attack discreet can minimize the financial losses and negative attention associated with it. Most companies would rather absorb the loss quietly than to have their reputations tarnished, which could negatively impact customer and stockholder confidence.

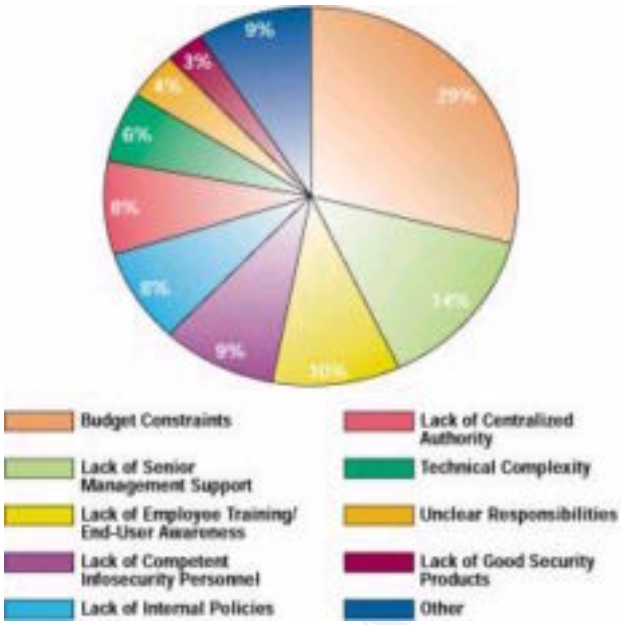
- High-tech companies have much to lose when stepping forward to expose an attack. They risk exposing closely held intellectual information possibly giving competitors an edge. Revealing such critical information could result in millions of dollars lost on research and development and could threaten the existence of the company.

- In some cases, embarrassment that such an attack occurred could silence an individual(s) whose primary responsibility was to prevent the attack in the first place. If it appears the damage is minimal, it is easier to patch the problem and not mention the incident at all than to call attention to weak performance.

- Laws are inadequate or non-existent and can't effectively address the tremendous explosion of cybercrimes across international borders. Additional governmental attention must be focused on extradition and mutual assistance treaties that will enable the United States to prosecute cybercrimes committed by international hackers and terrorists. [5]

Information Security Magazine released the results of a study to determine the greatest obstacles preventing businesses from providing adequate information security. *Figure 3* provides a realistic look at the reasons behind weak security spending.[12]

Computer Security Spending Issues -1999



http://www.securitystats.com/sspend.asp
Figure 3

Budget constraints, lack of senior management support, and lack of employment training/end-user awareness makes up 53% of the problem. Does your budget adequately support your security requirements?

National Response

Efforts are being made to raise awareness and combat the growing problem of cybercrime. Tolerance is fading and a new interest is emerging to create more secure environments. Laws are being created, new cyber-specific organizations are being established, special units are receiving high-tech training and companies are heeding sound advice and making effective changes. It is estimated that worldwide IT spending will reach 1.2 trillion in 2002. The United States will account for 572.8 billion, European countries - $326.6 billion, Asia/Pacific - $267.8 billion, and Latin American countries - 46.7 billion.[13]

The federal government is responding to increased network crimes with technical educational programs for college students. Students who contract to serve in the "CyberCorps" receive scholarships for an education in Information Technology and System Security. More than 200 students are taking advantage of the 8.6 million dollars of scholarship money. Each student receives an obligation of one-year service for each year of educational funding. Additional incentives will be necessary to retain the services of these valuable human resources as they near the end of their obligation. The goal is to infuse their expertise into federal agencies nationwide to protect the availability and integrity of our information resources. [14]

The United States Government is cracking down on federal agencies that are not compliant with basic security requirements as was shown when a court order forced the Department of Interior to disconnect from the Internet in December of 2001. The Bureau of Indian Affairs Chief Information Officer had become very concerned with lack of network security that was to protect millions of dollars in special trust funds for American Indians. His concern prompted a court appointed investigator who effortlessly broke into their system and was able to gather account holders' information and create new accounts. A federal judge ordered all computers providing access to Indian trust data be disconnected from the Internet. Seventy-one thousand employees in the Interior's 14 bureaus found themselves disconnected from the outside world. Although thousands of citizens were impacted, to include 40,000 American Indians who were counting on federal checks, the government shutdown continued until the court was satisfied all security measures were met. The federal government never wavered in their decision to shut down one of its very own agencies. It took approximately three months before all 14 Bureaus were gradually allowed to reconnect.[15] Despite this unprecedented act, there are smaller agencies with similar vulnerabilities continuing to operate under the radar of detection. All agencies, regardless of size or mission, will eventually be held to the same standards.

Detecting and prosecuting cybercriminals takes specially trained law enforcement agents. The federal government is developing specific task forces and special agencies to do just that. Unique training is necessary for securing evidence and the interrogation of suspects. Each officer must stay current with the latest technology and developments in order to understand and thoroughly investigate security crimes.[9]

The National Infrastructure Protection Center (NIPC) was created in February of 1998. This Federal agency's mission is to serve as the federal focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures. NIPC realized the importance of an alliance between state and private organizations to facilitate the sharing of information and sponsored 'InfraGard'. This federal initiative enhances information sharing and two-way communication to expose incidents of intrusions and vulnerabilities associated with them.[16] It encourages companies to report system compromises without risk of public disclosure. InfraGard is gaining momentum nationally.

Software developers such as Microsoft are eager to release their new technology before they have had a chance to fully test and discover its vulnerabilities. A competitive industry and the race to gain market positions prompts developers to release their products with the intent to 'fine-tune' it after it hits the marketplace. Today's consumers are now demanding security in addition to functionality in software products and developers are beginning to listen.

A wealth of government and public resources and tools are available at your fingertips. These resources can make the process of securing your systems a little easier. Throughout my research, I have discovered several valuable web sites worth mentioning. They include

a broad spectrum of security concerns to include: incident response and reporting, advisories, various discussion groups, forensic groups, incident groups, newsgroups, anti-virus upgrades, virus hoaxes and myths, penetration testing – tools - techniques - reports – discussions, laws and policies, and a clearinghouse of computer crime investigations.

www.fedcirc.gov, www.nipc.gov, www.cybercrime.gov, www.ciac.org, www.nai.com,

www.infragard.net, www.securityfocus.com, www.techrepublic.com, www.cert.org,

http://hoaxbusters.ciac.org, www.vmyths.com, www.atstake.com, http://csrc.nist.gov

The United States Congress has taken steps to define cybercrime. Recent legislation greatly enhances global policing of the Internet. Ongoing law enforcement efforts are becoming increasingly effective, but without legislation, prosecution could not easily cross international borders. Congress and the International community have moved swiftly to provide a series of substantive laws focusing on protecting global Internet transactions. . Five recent bills address the following cybercrime areas: the strengthening of foreign protection measures (High Tech Crime Bill S.2092), increased international jurisdiction (Internet Security Act of 2000 S.2430), establishment of laws focused on juvenile perpetrators under 18 years of age (Internet Integrity and Critical Infrastructural Protection Act of 2000 S.2448), increased penalties for computer fraud (S.2451), and finally the establishment of an organization to act as a focal point for law enforcement programs and training (Law Enforcement Science and Technology Act of 2000 H.R. 4403). These bills will create the solid framework governing global networking.[6]

In 1998, the Information Assurance Vulnerability Alert (IAVA) process was instituted. It was designed to manage "positive control of vulnerability notification and corresponding corrective action" within the Department of Defense. The Defense Information Systems Agency (DISA) manages the IAVA process and distributes alerts within DoD. All DoD agencies are required to register their system assets with the Vulnerability Compliance Tracking System (VCTS) thus ensuring patches for known vulnerabilities have been applied.[17]

Knowledge is the driving force behind change. We are slowly becoming aware of the problems plaguing our networks and many new initiatives are actively addressing and combating the proliferation of cybercrime. Although the results are visible, it will take a tremendous effort above and beyond what has currently been done before we can claim success.

Conclusion

Today, everyone is exposed to potential attacks and has a responsibility to its network neighbors to minimize their own vulnerabilities in an effort to provide a more secure and stable network. As the enormity of the problem unfolds, we will better comprehend how vital it is to work towards dramatic changes in research, prevention, detection and reporting, and computer crime investigation. Security can no longer be thought of as an impediment to accomplishing the mission, but rather a basic requirement that is properly resourced.

Our focus has been to implement the newest and most advanced technology, but little has prepared us for the gaping security holes we've neglected to mend along the way. From the ranks of management to every employee that works behind each terminal, the policies that protect and mitigate risks must be current, understood, and aggressively enforced. Reporting must be standard operating procedure so that everyone can realize the total impact of cybercrime and define what is required for a secure cyber environment. The responsibility belongs to everyone and it is with that effort we will be able to harness the security of this new technological age. An enormous challenge lies before us and we must attack it with the same enthusiasm and determination that brought us to this new frontier.

REFERENCES

[1]Rapalus, Patrice. "Cyber Crime Bleeds U.S. Corporations for Third Year in a Row". April 7, 2002. http://www.gocsi.com/press/20020407.html

[2]San Diego Police Department. "Computer Crime – Tips for Businesses". May 2002. http://www.sannet.gov/police/prevention/computer.shtml

[3]CERT and CERT Coordination Center. "CERT/CC Statistics 1988-2002". April 5, 2002. http://www.cert.org/stats/cert_stats.html

[4]The National Fraud Center, Inc. "The Growing Global Threat of Economic and Cyber Crime" (PDF) December 2000. http://www.lexisnexis.com/risksolutions/conference/docs/cyber.pdf

[5]CRYPTEK. "Network Security From the Inside Out". (PDF) May 2002. http://www.cryptek.com/Company/presskit/corporate.pdf.

[6]DeLong, Daniel F. "U.S. Falling Behind in Cyber Combat". June 1, 2001. http://www.ecommercetimes.com/perl/story/10193.html

[7]Waite, Beverly. "The Computer Economics Security Review 2002". April 2, 2002. http://www.computereconomics.com/article.cfm?id=356

[8]Business Wire. "Employee Computer Crime – From Petty Theft to Grand Larceny". Jan. 16, 1998. http://www.infowar.com/class_2/class2_012198a.html-ssi

[9]Miller, Brian. "Computer Crime Requires Virtual Patrol". March 1995. http://www.govtech.net/magazine/gt/1995/mar/compcrim.phtml

[10] Raman, Prasanna. "Laws to Deal with Computer Crimes". July 12, 2001. http://www.niser.org.my/news/2001_07_12_01.html

[11]Associated Press. "Survey: Hacking Often Unreported". 2002. http://www.msnbc.com/news/735198.asp

[12]Information Security Magazine. "Computer Security Spending Statistics". July 1999. http://www.infosecuritymag.com/articles/1999/enough.shtml

[13]Waite, Beverly. "Worldwide IT Spending Will Reach $1.2 Trillion in 2002". May 1, 2002. http://www.computereconomics.com/article.cfm?id=538

[14]Sausner, Rebecca. "U.S. Seeks a Few Good Cyber-Cops". May 23, 2001. http://www.ecommercetimes.com/perl/story/9960.html

[15]Friel, Brian. "BLACKOUT". Government Executive. May 1, 2002. http://www.govexec.com/features/0502/0502s1.htm

[16]InfraGard. "InfraGard – Capital of Texas Chapter". Web site. (May 2002).
http://www.infragard-austin.org

[17]National Communications System Telecommunications Speech Service, Volume IV, Number 14. Prepared Statement of Major General James D. Bryan. May 2001.
http://www.ncs.gov/N5_HP/Customer_Service/XAffairs/SpeechService/2001/SS01-014.htm

Chuvakin, Anton. "Insider Attacks: The Doom of Information Security". Copyright 2001.
http://www.sinc.sunysb.edu/Stu/achuvaki/internal-attacks.html

Cosmiverse staff writer. "FBI Says Hacking Is Up". April 8, 2002.
http:/www.cosmiverse.com/tech04080202.html

InfraGard Home Page. "Guarding the Nation's Infrastructure". (May 2002).
http://www.infragard.net

O'Brien, Karen. "Hacker, Cracker, and Internet Security". April 2001.
http://www.umm.maine.edu/BEX/students/KarenO'Brien/ko310.html

Sjoholm, Hans. SearchSecurity.Com "Definition – Cracker". October 1999.
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211852,00.html

FOLDOC. Free On-line Dictionary of Computing. (April 2002).
http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?query=hacker&action=Search