MR. KEVIN MITNICK

Honorable Chairperson Thompson, Distinguished Senators, and Members of the Committee:

My name is Kevin Mitnick. I appear before you today to discuss your efforts to create legislation that will ensure the future security and reliability of information systems owned and operated by, or on behalf of, the federal government.

I am primarily self-taught. My hobby as an adolescent consisted of studying methods, tactics, and strategies used to circumvent computer security, and to learn more about how computer systems and telecommunication systems work.

In 1985 1 graduated cum laude in Computer Systems and Programming from a technical college in Los Angeles, California, and went on to successfully complete a post-graduate project in designing enhanced security applications that ran on top of a computer's operating system. That post-graduate project may have been one of the earliest examples of "hire the hacker" the school's administrators realized I was hacking into their computers in ways that they couldn't prevent, and so they asked me to design security enhancements that would stop others' unauthorized access.

I have 20 years experience circumventing information security measures, and can report that I have successfully compromised all systems that I targeted for unauthorized access save one. I have two years experience as a private investigator, and my responsibilities included locating people and their assets using social engineering techniques.

My experience and success at accessing, and obtaining information from computer systems first drew national attention when I obtained user manuals for the COSMOS computer systems (Computer Systems for Mainframe Operations) used by Pacific Bell.

Ten years later the novel "Cyberpunk" was published in 1991, which purported to be a "true" accounting of my actions that resulted in my arrest on federal charges in 1988. One of the authors of that novel went on to write similarly fictionalized "reports" about me for the New York Times, including a cover story that appeared July 4, 1994. That largely fictitious story labeled me, without reason, justification, or proof, as the "world's most wanted cybercriminal." Subsequent media reports distorted that claim into the false claim that I was the first hacker on the FBI's "Ten Most Wanted" list. That false exaggeration was most recently repeated during my appearance on CNN's Burden of Proof program on February 10, 2000. Michael White of the Associated Press researched this issue with the FBI, and FBI representatives denied ever including me on their "Ten Most Wanted" list.

I have gained unauthorized access to computer systems at some of the largest corporations on the planet, and have successfully penetrated some of the most resilient computer systems ever developed. I have used both technical and non-technical means

to obtain the source code to various operating systems and telecommunications devices to study their vulnerabilities and their inner workings.

After my arrest in 1995, 1 spent years as a pretrial detainee without benefit of bail, a bail hearing, and without the ability to see the evidence against me, combined circumstances which are unprecedented in U.S. history according to the research of my defense team. In March of 1999 1 pled guilty to wire fraud and computer fraud. I was sentenced to 68 months in federal prison with 3 years supervised release.

The supervised release restrictions imposed on me are the most restrictive conditions ever imposed on an individual in U.S. federal court, again according to the research of my defense team. The conditions of supervised release include, but are not limited to, a complete prohibition on the possession or use, for any purpose, of the following: cell phones, computers, any computer software programs, computer peripherals or support equipment, personal information assistants, modems, anything capable of accessing computer networks, and any other electronic equipment presently available or new technology that becomes available that can be converted to, or has as its function, the ability to act as a computer system or to access a computer system, computer network, or telecommunications network.

In addition to these extraordinary conditions, I am prohibited from acting as a consultant or advisor to individuals or groups engaged in any computer-related activity. I am also prohibited from accessing computers, computer networks, or other forms of wireless communications myself or through third parties.

I was released from federal prison on January 21, 2000, just 6 weeks ago. I served 59 months and 7 days, after earning 180 days of time off for good behavior. I am permitted to own a land line telephone.

Computer Systems and Their Vulnerabilities

The goal of information security is to protect the integrity, confidentiality, availability and access control to the information. Secure information is protected against tampering, disclosure, and sabotage. The practice of information security reduces the risk associated with loss of trust in the integrity of the information.

Information security is comprised of four primary topics: physical security, network security, computer systems security, and personnel security. Each of these four topics deserves a complete book, if not several books, to fully document them. My presentation today is intended to provide a brief overview of these topics, and to present my recommendations for the manner in which the Committee may create effective legislation.

1. Physical Security

1.1 Uncontrolled physical access to computer systems and computer networks dramatically increases the likelihood that the system can and will suffer unauthorized access.

1.1.1 Hardware Security

May be locked in rooms or buildings, with guards, security cameras, and cypher-controlled doors. The greatest risk to information security in apparently secure hardware environments is represented by employees, or impostors, who appear to possess authorization to the secured space.

1.1.2 Data Security

Government agencies require formal backup procedures to ensure against data loss. Equally stringent requirements must be in place to ensure the integrity and security of those backup files. Intruders who cannot gain access to secure data but who obtain unauthorized access to data backups successfully compromise any security measures that may be in place, and with much less risk of detection.

2. Network Security

2.1 Stand-alone computers are less vulnerable than computers that are connected to any network of any kind. Computers connected to networks typically offer a higher incidence of misconfiguration, or inappropriately enabled services, than computers that are not connected to any network. The hierarchy of network "insecurity" is as follows:-- Stand-alone computer - least vulnerable

-- Computer connected to a LAN, or local area network - more vulnerable

-- Computer and a LAN accessible via dial-up - even more vulnerable

-- Computer and LAN connected to internet - most vulnerable of all

2.1.1 Unencrypted Network Communications

Unencrypted network communications permit anyone with physical access to the network to use software to monitor all information traveling over the network, even though it's intended for someone else. Once a network tap is installed, intruders can monitor all network traffic, and install software that enables them to capture, or "sniff," passwords from network transmissions.

2.1.2 Dial-in Access

Dial -in access increases vulnerabilities by opening up an access point to anyone who can access ordinary telephone lines. Off site access increases the risk of intruders gaining access to the network by increasing the accessibility of the network and the remote computer.

3. Computer Systems Security

3.1 Computer systems that are not connected to any network present the most secure computing environment possible. However, even a brief review of standalone computer systems reveals many ways they may be compromised.

3.1.1 Operating Systems

The operating systems control the functions of the computer: how information is stored, how memory is managed, and how information is displayed -- it"s the master program of the machine. At its core, the operating system is a group of discrete software programs that have been assembled into a larger program containing millions of lines of code. Large modern day operating systems cannot be thoroughly tested for security anomalies, or "holes," which represent opportunities for unauthorized access.

3.1.2 Rogue Software Programs

"Rogue" software applications can be installed surreptitiously, or with the unwitting help of another. These programs can install a "back door", which usually consists of programming instructions that disable obscure security settings in an operating system and that enable future access without detection; some back door programs even log the passwords used to gain access to the compromised system or systems for future use by the intruder.

3.1.3 Ineffective Passwords

Computer users often choose passwords that are in the dictionary, or that have personal relevance, and are quite predictable. Static, or unchanging, passwords represent another easy method for breaching a computer system -- once a password is compromised, the user and the system administrators have no way of knowing the password is known to an intruder. Dynamic passwords, or non-dictionary passwords are problematic for many users, who write them down and keep them near their computers for easy access -- their own, or anyone who breaches physical security of the computer installation.

3.1.4 Uninstalled Software Updates

Out-of-date system software containing known security problems presents an easy target to an intruder. Systems administrators cannot keep systems updated as a result of work overload, competing priorities, or ignorance. The weaknesses of systems are publicized, and out-of-date systems typically offer well-known vulnerabilities for easy access.

3.1.5 Default Installations

Default installations of some operating systems disable many of the built-in security features in a given operating system. In addition, system administrators unintentionally

misconfigure systems, or include unnecessary services that may lead to unauthorized access. Again, these weaknesses are widely publicized within the computing community, and default or misconfigured installations present an easy target.

4. Personnel Security

4.1 The most complex element in information security is the people who use the systems in which the information resides. Weaknesses in personnel security negate the effort and cost of the other three types of security: physical, network, and computer system security.

4.1.1 Social Engineering

Social engineering, or "gagging," is defined as gaining intelligence through deception. Employees are trained to be helpful, and to do what they are told in the workplace. The skilled social engineer will use these traits to his or her advantage as they seek to gain information that will enable them to achieve their objectives.

4.1.2 Email Attachments

Email attachments may be sent with covert code embedded within. Upon receiving the email, most people will launch the attachment, which can lower the security settings on the target machine without the user's knowledge. The likelihood of a successful installation using this method can be increased by following up the email submittal with a telephone call to prompt the person to open the attachment.

Information Security Exploits

Information security exploits are the methods, tactics, and strategies used to breach the integrity, confidentiality, availability or access control of information. Discovery of compromised information security has several consequences, the most important of which is the decline in the level of trust associated with the compromised information and systems that contain that information. Examples of typical security exploits follow.

5. Physical Security Exploits

5.1 Data Backup Exploit Using deception or sheer bravado, the intruder can walk into the off site backup storage facility, and ask for the physical data backup by pretending to be from a certain agency. The intruder can claim that particular backup is necessary to perform a data restoration. Once an intruder has physical possession of the data, the intruder can work with the data as though he possessed superuser, or system administrator, privileges.

5.2 Physical Access Exploit

If an intruder gains physical access to a computer and is able to reboot it, the intruder can gain complete control of the system and bypass all security measures. Ali extremely

powerful exploit, but one that exposes the intruder to great personal risk because they're physically present on the premises.

5.3 Network Physical Access Exploit

Physical access to a network enables an intruder to install a tap on the network cable, which can be used to eavesdrop on all network traffic. Eavesdropping enables the intruder to capture passwords as they travel over the network, which~will enable full access to the machines whose passwords are compromised.

6. Network Security Exploits

6.1 Network software exists that probes computers for weaknesses. Once one system weaknesses are revealed and the system is compromised, the intruder can install software (called "sniffer" software) that compromises all systems on the network. Following that, an intruder can install software that logs the passwords used to access that compromised machine. Users routinely use the same or similar passwords across multiple machines; thus, once one password for one machine is obtained, then multiple machines can be compromised (see "Personnel Security Exploits").

7. Computer System Exploits

7.1 Vulnerabilities in programs (e.g., the UNIX program sendmail) can be exploited to gain remote access to the target computer. Many system programs contain bugs that enable the intruder to trick the software into behaving in a way other than that which is intended in order to gain unauthorized access rights, even though the application is a part of the operating system of the computer.

7.2 A misconfigured installation on a computer in operation at the Raleigh News and Observer, a paper in Raleigh, North Carolina, demonstrates the problematic aspect of system misconfiguration. Using the UNIX program "Finger," which enables one to identify the users that are currently logged into a computer system, I created a user name on the computer system I controlled. The user name I assigned myself matched exactly the user name that existed on the target host. The misconfigured system was set to"trust"' any computer on the network, which left the entire network open for unauthorized access.

8. Personnel Security Exploits

8.1 Social Engineering -- involves tricking or persuading people to reveal information or to take certain actions at the behest of the intruder. My work as a private investigator relied heavily on my skills in social engineering.

In my successful efforts to social engineer my way into Motorola, I used a three-level social engineering attack to bypass the information security measures then in use. First I was able to convince Motorola Operations employees to provide me, on repeated occasions, the pass code on their security access device, as well as the static PIN. The

reason this was so extraordinary is that the pass code on their access device changed every 60 seconds: every time I wanted to gain unauthorized access, I had to call the Operations Center and ask for the password in effect for that minute.

The second level involved convincing the employees to enable an account for my use on one of their machines, and the third level involved convincing one of the engineers who was already entitled to access one of the computers to give me his password. I overcame that engineer's vigorous reluctance to provide the password by convincing him that I was a Motorola employee, and that I was looking at a form that documented the password that he used to access his personal workstation on Motorola's network -- despite the fact that he never filled out any such form! Once I gained access to that machine, I obtained Telnet access to the target machine, access which I had sought all along.

8.2 Voice Mail and Fax Exploit

This exploit relies on convincing an employee at a large company to enable a voice mailbox: the intruder would call the people who administer the voice mailboxes for the target company and request a mailbox. The pretext would be that the intruder works for a different division, and would like to retrieve messages without making a toll call.

Once the intruder has access to the voice mail system, the intruder would call the receptionist, represent himself as an employee of the company, and ask that they take messages for him; last but not least, the intruder would request the fax number and ask that incoming faxes be held for pickup. This sets the stage for the call to the target division of the company.

At this point, the intruder would call the target division to initiate the fax exploit with the goal of obtaining the targeted confidential company information. During that call the intruder would identify himself as an employee of the division whose voice mail and fax systems have just been compromised, he would cite the voice mail box in support of his identity, and would social engineer the target employee into faxing the target information to the compromised fax number located at one of their other offices.

Now the intruder would call the receptionist, tell the receptionist that he's in a business meeting, and ask that the receptionist fax the confidential material "to the hotel." The intruder picks up the fax containing confidential information at the secondary fax, which can-not be traced back to either the intruder or the targeted company.

I used this exploit to successfully compromise ATT's protected network access points routinely. ATT had learned that a system had been compromised by unauthorized entry at a central network access point called "DataKit." They imposed network access passwords on all DataKits to inhibit unauthorized access. I contacted one of the manager's secretaries and used the Fax Exploit to convince the secretary to fax me the password that enabled access to a DataKit that controlled dial-up access to ATT's worldwide computer network.

9. Recommendations

The Voice Mail and Fax Exploit demonstrates the most important element in my testimony today: that verification mechanisms are the weak link in information security, and voice mail and fax are the tools used to verify the authenticity of the credentials presented by someone seeking physical, network, or computer systems access.

The methods that will most effectively minimize the ability of intruders to compromise information security are comprehensive user training and education. Enacting policies and procedures simply won't suffice. Even with oversight the policies and procedures may not be effective: my access to Motorola, Nokia, ATT, Sun depended upon the willingness of people to bypass policies and procedures that were in place for years before I compromised them successfully. The corporate security measures that I breached were created by some of the best and brightest in the business, some of whom may even have been consulted by the committee as you drafted your legislation, Senate Bill S1993.

S1993 is represents a good first step toward the goal of increasing information security on government computer systems. I have several recommendations that I hope will increase the effectiveness of your bill.

1. Each agency perform a thorough risk assessment of the assets they want to protect.

2. Perform a cost-benefit analysis to determine whether the price to protect those systems represents real value.

3. Implement policies, procedures, standards and guidelines consistent with the risk assessment and cost benefit analyses. Employee training to recognize sophisticated social engineering attacks is of paramount importance.

4. After implementing the policies, procedures, standards and guidelines, create an audit and oversight program that measures compliance throughout the affected government agencies. The frequency of those audits ought to be determined consistent with the mission of a particular agency: the more valuable the data, the more frequent the audit process.

5. Create a numeric "trust ranking" that quantifies and summarizes the results of the audit and oversight programs described above. The numeric "trust ranking" would provide at-a-glance ranking -- a report card, if you will -- of the characteristics that comprise the four major categories defined above: physical, network, computer systems, and personnel.

6. Effective audit procedures -- implemented from the top down -- must be part of an appropriate system of rewards and consequences in order to motivate system administrators, personnel managers, and government employees to maintain effective information security consistent with the goals of this committee.

Conclusion

Obviously a brief presentation such as the one I've made today cannot convey adequately the measures needed to implement effective information security measures. I'm happy to answer any questions that may have been left unanswered for any members of the Committee.