INSTITUTE FOR
CRIMINAL JUSTICE
EDUCATION

ICJE, P.O. Box 293, Montgomery, AL 36101 * 334-280-0020

ICJE Feature Article, May 28, 2002

Preparing for Cyberattacks

Adapted from *A Survey of Terrorism, 2002 Edition*
Published May, 2002 by ICJE, Inc.
Copyright 2002, 136 pp.
Paper
ISBN 0-9704088-1-1

Robert T. Thetford, J.D.

The Future

A recent analysis of past cyberattacks makes some ominous predictions for the near future as the U.S. engages in its war on terrorism:[1]

Electronic information sites in the U.S. and allied countries will be exposed to increasing attempts at defacing for the purpose of spreading disinformation and propaganda.

Denial of Service (DoS) attacks [2] will increase, as will the use of worms and viruses.

Unauthorized intrusions into U.S. systems and networks will result in critical infrastructure outages and corruption of vital data.

As a nation, we must understand that the threat of cyberterrorism is real, that it is already occurring, and that massive attacks are probable in the future. Only when we fully understand how fragile our critical computer infrastructure is and how vulnerable our systems are to both inside and outside attack will we take the steps necessary to protect our business and governmental structures. Even then we are preparing to fight the last war due to the ever increasing ingenuity of cybercriminals, cyberterrorists and state supported cyberwarfare planners.

Preparation for the Attack

If one assumes that a future cyberattack is likely in some form, what are the steps, if any, which may be taken to protect networked governmental, corporate or even home computer systems? First and foremost, learn from other's mistakes by undertaking the following specific steps:

- **Policy review**

Every government and virtually every business in the United States now has at least one computer system. If employees have access to computers and systems, a review should be immediately taken of the current practices and procedures to determine appropriate use of network resources. Who has access and to which systems? What is their level of access? Exactly what are employees able to do with their access? Are written policies in place? Are they enforced? Policy reviews should address e-mail and Internet use as well as basic security practices. There are many sample policies available and numerous reputable companies in existence that conduct security audits. Much of what they do is plain common sense, but is generally based upon known methods of intrusion. If your organization is contemplating the use of a physical/technology security service for a review of your procedures, insure that those who conduct the audit have ample experience in their fields - in other words, use the best people you can find. Once policies are written and/or upgraded, they should be implemented as part of normal training, and every employee should acknowledge the receipt of training by signature.

After review by appropriate legal counsel, consideration should be given to the use of an on-system warning screen advising the user that the system confers no privacy rights and is to be used by authorized personnel only for official government/company business. Users should be notified that the system is subject to being monitored for appropriate use (perhaps defining the term “appropriate use”). The warning should further advise that system resources are subject to being retained and reviewed by the government/company and may be furnished to others, including law enforcement agencies, at the discretion of the government/company. Finally, users should be notified that by using the system they understand and consent to the provisions of the warning.**(3)** If not placed in a warning screen, the above should be incorporated into the government/company policy and should be acknowledged by all employees having access to system resources.

- **Firewalls and Virus Checkers**

Computers and networks without operating firewalls and up-to-date virus protection are similar to open entrance doors in homes - they are invitations for criminals to enter, steal and vandalize.

Firewalls are generally considered necessary when using “always on” connections like T1 lines, cable and DSL connections because a typical telephone modem for a home line uses a different computer address (URL) each time the server is dialed. To test a particular computer's vulnerability to outside probes, run the tests at Gibson Research (https://grc.com/x/ne.dll?bh0bkyd2), or at the Symantec site, (http://www.symantec.com/securitycheck/). These will show the need for firewall protection or will show how much protection an existing firewall offers. One additional bonus for firewalls that should not be overlooked is the filtering capacity that they offer. Most provide filtering options ranging from no filtering to totally paranoid, and site-blocking features prevent most (but not all) unauthorized site visits. E-mail programs provide the same provision for blocking unwanted e-mail, but their ability to filter is somewhat limited.

Virus checkers are relatively cheap and offer substantial protection from e-mail and Web viruses, but must be frequently updated to be effective. The once laborious process of updating has been simplified and now is easily accomplished through automatic updates or one-button clicks.

Most virus protection software is based on pattern recognition of known virus characteristics. Since these recognition patterns are developed only after new viruses are identified, they are unable to prevent new and unrecognized viruses. Because no virus checking software offers 100 percent protection, an examination of company computer operating policies should be mandatory with a goal of limiting Internet access to only those employees who have a need for Internet use in their jobs. E-mail use also should be examined and policies formulated to restrict the receipt of attachments, which often contain viruses. Thought should be given to notifying employees that their e-mail usage is subject to being monitored (they should sign a statement of acknowledgment) and then periodically examine e-mail content for inappropriate or excessive usage. Finally, a retention period for e-mail messages should be established to decrease storage requirements and incidental exposure. This period should be more than 30 days but less than a year. The ability to retrieve e-mail messages may become extremely important in the event that a cyberattack or virus renders the system inoperable.

- **Password Protection**

Individuals generally resist having to bother with passwords and when forced to do so, they often pick common words that are easily determined by scanning computers. To be safe, passwords should be a combination of letters and numbers and should be changed often. It is also a mistake to leave passwords in easily accessible places, such as under mouse pads or taped to the back of computers.

- **Security Patch Updates**

Many attacks could be thwarted simply by installing system patches provided by software manufacturers to plug known security breaches. Network administrators and individuals should check system vendor sites often for upgrades designed to repair system deficiencies.

Along the same lines, administrators should frequently check the FBI's National Infrastructure Protection Center (http://www.nipc.gov/) site and Carnegie Mellon University's CERT Coordination Center site, a federally funded research site located at (http://www.cert.org/) for updated cyberattack information. The CERT site is particularly helpful for home computer users as it offers practical tips in non-technical language.

The National Infrastructure Protection Center (NIPC) also provides a forum (InfraGard) which encourages the exchange of information between the U.S. Government and private sector members. NIPC acts as a facilitator to its members through the dissemination and exchange of information about infrastructure protection. InfraGard may be accessed through the NIPC site above or directly through http://www.infragard.net.

- **Data Backup**

One of most common complaints among computer users involves system crashes, whether they are caused by a virus, sabotage or malfunction. Other than virus protection, the easiest and cheapest way to protect a system is through periodic data backups. Most home users and small businesses, however, seldom backup their data on a frequently scheduled basis, and when the crash comes, which it inevitably does, weeks or months of work can be lost. Nor is it enough to simply copy the data. Provisions should be made to store the data at a secure off-site location for fire and theft protection. Backup procedures and schedules should be thoroughly covered in the governmental or company policy or procedure manual. In addition to electronic data backup, vital hard copy files should also be achieved for the unlikely event that extended power or computer outages might occur. Protection against transient power outages should be provided by UPS battery backup systems to eliminate unnecessary down time, with thought given to implementing generator-supplied power supply for the entire computer system.

- **Internal Security**

Finally, because most of the computer attacks today, including vandalism and theft, still originate from within organizations, internal security must be given more consideration. Information technology training, security education and employee screening are all tools used to safeguard against internal attacks and theft. Periodic security audits from trusted outside agencies (discussed above), offer an unbiased view of the level of protection offered, as well as providing notice to company employees that infractions will likely be discovered and appropriate sanctions imposed.

While preventing all cyberattacks is impossible, with some basic planning and security awareness in mind, there are definite steps that companies, agencies and individuals can take to prepare their systems and personnel for the challenge. Failing to take these basic steps outlined above is akin to playing Russian roulette. Disaster may not strike immediately, but statistically it is bound to occur. What will you (or your organization) do when it does?

- **PDA Security**

Often overlooked is the absolute vulnerability of Personal Digital Assistants (PDAs) such as Palm Pilots and similar devices. Because of their ease of use, employees frequently place sensitive information, including organizational and personal information in their PDAs. With the increase in memory capabilities, entire databases and volumes of information may be quickly downloaded from computers to the PDA, causing enormous individual and organizational security risks. At least one security firm believes that entire networks could be vulnerable because the usual passwords don't protect data held on Palm PDAs.**(4)**

With the use of PDA growth estimated at more than 50 per cent in the next few years, organizations should immediately review security policies to include restricted PDA use and security training. Further, access control systems and encryption devices should be installed on all PDAs, and periodic audits scheduled to insure compliance.

Conclusion

Many, if not most, businesses and governmental entities are on tightly restricted computer system budgets. Systems are expensive to purchase and maintain, especially with such a limited effective lifespan. If corners are to be cut, it is often in the systems security and training areas. In light of the current threats, policy makers should carefully reconsider this view by asking one simple question: Just how much damage could be inflicted on my organization in a worst-case scenario attack on our computer system(s)? If a realistic initial appraisal determines a high level of vulnerability for continued operation, serious consideration should be given toward an immediate and thorough review of the organization's information technology security. This security review can be implemented using the bullet point topics in the preceding section as guideposts. The review should begin with a policy review, and after inspection and corrective action on the other items have been completed, the policy should again be examined to insure all necessary changes have been incorporated.

It is not enough to make system and policy changes, however. All personnel (not just systems personnel) must be given adequate training in physical security, threat analysis, and emergency operations to insure that they understand likely threats and know what actions (including reporting procedures) to take in the event of a threat. In addition, computer systems personnel should be continuously trained in protection methods as outlined above and should be encouraged to be alert for potential violations and security breaches. The key to this training is to realistically portray the threat so that each employee understands his/her role in protecting both employees and the organization.

All personnel must understand that the likelihood of serious security breaches is now at such an increased level that their continued employment and possibly their physical safety depend upon compliance with organizational policy and threat consciousness. Security infractions and breaches must be thoroughly investigated and corrective action immediately taken, to include after-action reviews so that violations are not repeated. Employees should be encouraged to report violations, and inadvertent breaches should not be punished if reported. The idea is to prevent mistakes or violations from being buried through fear of reprisal rather than being reported and corrected.

Not all of the above suggestions are expensive. Many can be accomplished “in house,” and with a minimum of effort. All systems should be reviewed immediately, however, as we are faced with dangers never before seen. President Bush advised following the September 11 attacks that we would most likely be engaged in a long war against very determined terrorists. Based upon the available evidence, those who have proclaimed themselves to be our enemies are well prepared. Are we?

Footnotes

1. Michael A. Vatis, “Cyber Attacks During the War on Terrorism,” Institute for Security Technology Studies at Dartmouth college, 9/22/01, <http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf> 10/1/01.
2. In a DoS attack, a computer (or a group of computers in the case of an organized attack) is directed to flood the target system with e-mail or requests for information. A DDoS attack accomplishes the same goal using captured, third party computers. In this type of attack, third party computer systems (called Zombies) are in essence hijacked and used to flood the target system with requests for information or e-mails, thereby totally overwhelming the target system and shutting it down for commercial traffic.
3. William C. Boni and Gerald L. Kovacich, I-Way Robbery, Crime on the Internet, (Boston:Butterworth-Heinemann, 1999), p. 166.
4. Aoife White, “Palm PDA threat to network security,” *Network News,* 3/15/01, <http://www.vnunet.com/News/1119214> 5/27/02.

ICJE articles have been prepared for educational and information purposes only. They are not intended to be published as legal advice or legal opinion about any specific subject matter. Transmission of this ICJE information is not intended to create, and receipt does not constitute, a lawyer-client relationship between the author(s), ICJE and the reader. The opinions expressed in the articles found herein are those of the author (s), and not necessarily those of ICJE. Officers and departments should review any proposed change in policy or procedure with the appropriate professional authority or advisor prior to implementation. All articles may be reproduced and distributed free of charge with attribution.