Privacy and Computer Security: Nine Questions

Kevin FitzGerald

This issue of *Popular Government* has devoted much attention to the legal parameters on sharing and protecting private information. Of equal importance is the security of information technology systems that store and convey sensitive information. This article poses nine straightforward questions for government officials to consider in assessing the security of their systems.

There is little doubt that information technology provides critical support for the delivery of government services. Although direct expenditures for technology often represent less than 2 percent of a local government's budget, the reach of technology extends to practically every government service. It is hard to imagine delivering services without the assistance of computer technology.

Local governments, large and small, support a vast array of computer hardware and software systems. They exchange public and private information via the Internet and a variety of "secure" networks among fellow employees, citizens, clients, and other governments. All expect information systems to do the work they were designed to do, be available when they are needed, and maintain the reliability and the integrity of the information that is contained within them.

The importance of security is heightened, and security is made more difficult, as an increasing number of people connect to public information systems. More and more, citizens and employees expect Web-based access to

The author is the director of the Center for Public Technology at the Institute of Government. Contact him at kfitz@iogmail.iog.unc.edu.

Dedicated personnel help keep local government computer systems secure.

numerous public services twenty-four hours a day. Also, the technology supporting these connections is diversifying as many governments invest in applications that rely on high-speed Internet connections and support a wide variety of wired, optical, and wireless equipment.

These developments require a security strategy that keeps pace with change while maintaining the fundamental requirements of data integrity. And make no mistake: there are daily threats to data integrity. The viruses (see the glossary, this page) that recently spread from Europe to every corner of the world, destroying billions of dollars' worth of information and erasing countless files, are a spectacular example of the damage that hackers can cause. The 2001 FBI Computer Crime and Security Survey conducted by the Computer Security Institute ranked computer viruses, improper use of Internet connections, the theft of laptop computers, and unauthorized employee access to computer systems as the top four types of security attacks, with the cost per incident ranging from a few thousand dollars to fifty million.[1]

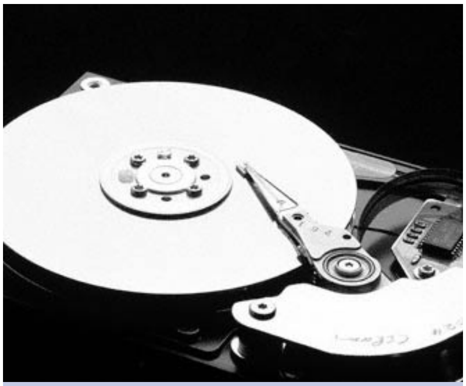
Clearly this is an issue that local officials cannot avoid. Here are nine questions to guide local governments in assessing their security vulnerabilities and in taking reasonable steps to mitigate unnecessary risk. (For helpful Web sites on computer security, see the sidebar on this page.)

Who in our organization is accountable for the security of information technology?

An organization should designate someone to be responsible and accountable for computer security. This often is a responsibility of the information technology director. The person should have sufficient technical training to do the job.

Do we have an information technology security plan?

There should be a written plan that is periodically reviewed and well communicated to management and employees. It should cover critical data policies, backup, disaster recovery, and user policies.



Glossary

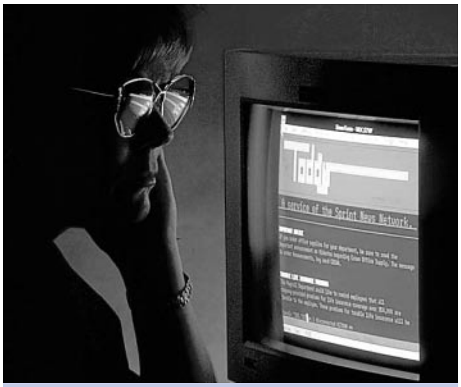
Disaster recovery plan: [A] plan maintained for emergency response, backup operations, and post-disaster recovery for an information system (IS), to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.

Firewall: [A] system designed to defend against unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

Patch: In a computer program, one or more statements inserted to circumvent a problem or to alter temporarily or permanently a usually limited aspect or characteristic of the functioning of the program, e.g., to customize the program for a particular application or environment.

Virus: 1. An unwanted program which places itself into other programs, which are shared among computer systems, and replicates itself. *Note:* A virus is usually manifested by a destructive or disruptive effect on the executable program that it affects. 2. Self-replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence.

Source: Telecom Glossary 2000, maintained by the U.S. National Telecommunications and Information Administration, available at http://www.its.bldrdoc.gov/projects/t1glossary2000/.



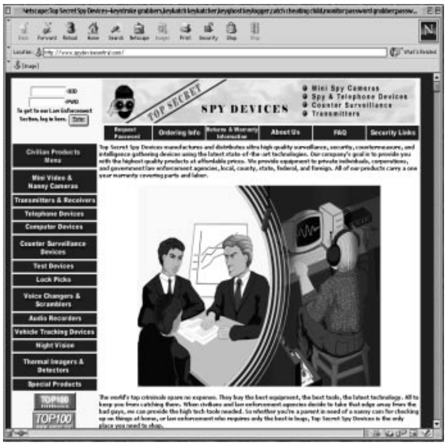
Helpful Links

Institute of Government, Center for Public Technology
http://www.cpt.unc.edu
The Center for Public Technology is a unit of the Institute of Government. Its mission is to assist North Carolina governments in making use of information technology to improve services and strengthen communities.

Top 20 Internet Security Vulnerabilities
http://www.sans.org/top20.htm
This site contains a listing of and information on twenty of the greatest Internet security vulnerabilities. It is maintained by the SANS (System Administration, Networking, and Security) Institute and the National Infrastructure Protection Center.

State of North Carolina Security Documentation
http://www.its.state.nc.us/Support/Security/Security.asp
This site contains information on the State of North Carolina's security plan. It is maintained by the North Carolina Office of Information Technology Services.

Glossary
http://www.its.bldrdoc.gov/projects/t1glossary2000/
The U.S. National Telecommunications and Information Administration maintains this searchable glossary.



Netscape: Top Secret Spy Devices–keystroke grabbers,keykatch keykatcher,keyghost keylogger,catch cheating child,monitor password grabber,passw...

http://www.spydevicecentral.com/

To get to our Law Enforcement Section, log in here.

Top Secret Spy Devices manufactures and distributes ultra high quality surveillance, security, countermeasure, and intelligence-gathering devices using the latest state-of-the-art technologies. Our company's goal is to provide you with the highest quality products at affordable prices. We provide equipment to private individuals, corporations, and government law enforcement agencies, local, county, state, federal, and foreign. All of our products carry a one year warranty covering parts and labor.

The world's top criminals spare no expense. They buy the best equipment, the best tools, the latest technology. All to keep you from catching them. When civilians and law enforcement agencies decide to take that edge away from the bad guys, we can provide the high tech tools needed. So whether you're a parent in need of a nanny cam for checking up on things at home, or law enforcement who requires only the best in bugs, Top Secret Spy Devices is the only place you need to shop.

Are our software licenses, patches (see the glossary), and various maintenance agreements up-to-date?

Software, equipment, and networks are continually modified. It is essential that these systems be kept up-to-date. Making sure that security provisions like firewalls (see the glossary) and virus software are current is especially important. A log of updates should be maintained. At times, virus definition files are updated several times a day. Servers and workstations should be set to download updates automatically and install the most current versions.

Is our security plan keeping up with our changing use of technology?

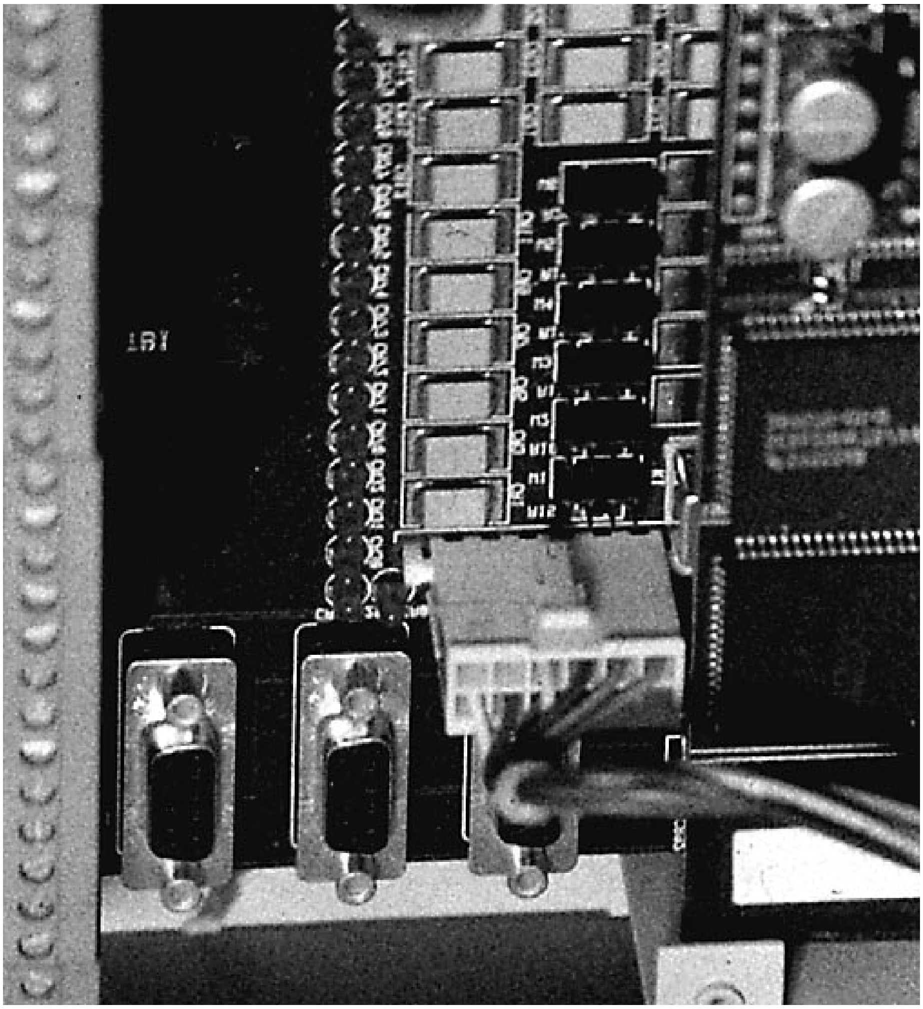
If there has been a recent upgrade in systems that changes traditional network configurations, the assumptions of the security plan must be reexamined to ensure that the plan has not been compromised.

Do we keep valuable equipment locked up?

Theft of equipment, especially laptop computers, can easily compromise sensitive information. Users whose laptops contain sensitive data should consider encrypting their hard drives to reduce the possibility of misuse.

How do we know if a hacker has gotten into our system or if data have been changed?

Software is available that is capable of detecting whether an unauthorized user has crossed the security perimeter. This information is helpful in understanding which systems are particularly vulnerable.



Do we have a disaster recovery plan (see the glossary) that is tested and capable of supporting operations without excessive loss of data?

Suppose a natural disaster destroys a unit's data center. Is the unit capable of restarting operations in a reasonable timeframe? Are backup tapes stored far enough off the site that they would survive a disaster such as a tornado? A government unit should consider negotiating a reciprocal agreement with another unit using the same hardware and software, whereby each would provide the other with emergency processing services.

What steps have we taken to train employees about security? Do employees know what is and is not acceptable behavior? Do they know where and how to report problems?

Clear written policy related to computer use and abuse is essential. This should be included in an employee's orientation.

Are we clear in our communications with citizens and clients about the security and the privacy of the information that is maintained?

Citizen confidence is critical. Citizens need to know what steps are being taken to ensure that private information is kept private.

Conclusion

Identifying what information is private is important. Ensuring that private information remains secure is just as important. Otherwise, privacy, and the confidence that citizens place in the custodians of the private information, may be compromised.

Note

[1] 2001 CSI/FBI Computer Crime and Security Survey (San Francisco, Cal.: Computer Security Inst., 2001), available at www.gocsi.com.