e-Sher®
Underwriting Managers
Protecting the Business of e-Business

News for You

Homeland "Cyber" Security: Protecting Your Company Against New Network Risks in a Post-September 11 World

By Philip Pierson,
Founder and Manager, e-Sher Underwriting Managers
Irvine, California

Since the September 11 attacks on the World Trade Center and the Pentagon, "security" has become an elusive goal. Safety measures have increased at our nation's airports and borders, but cyber space remains largely unregulated and vulnerable to terrorist infiltration and attack. Many security experts view this as an urgent danger requiring more time and attention to properly fend off future cyber terrorist activity. But in a survey conducted by Network World Magazine, 85 to 90 percent of IT professionals polled at large U.S. corporations said they were confident in the safety and security of their own networks.[1] Is this a false sense of safety?

September 11 has shown us the destructive force that ruthless determination, meticulous planning and systematic coordination can achieve, even without sophisticated nuclear, chemical or biological weapons. We have seen our airplanes converted into missiles aimed at our nation's icons; our mail and postal service utilized as a vehicle for bioterrorism. The question now posed is what other modes of modern life can be utilized to terrorists' advantage? Perhaps the Internet, e-mail and our nation's network infrastructure. This is a growing concern among officials that the next potentially deadly attack may be an act of cyber terrorism.

The Internet is a useful vehicle

There is no doubt that terrorists today are very technology savvy. Law enforcement officials said that the World Trade Center hijackers were very computer literate, communicating via encrypted email and using the Internet to help plot the September 11 events.[2]

[1] Bruce Francis, Kathleen Hays, "IT Security After Terrorist Attacks," *Market Impact*, CNNfn Transcript #102206cb.107, October 22, 2001.

[2] Richard Behar, "Fear Along the Firewall: America's computer databases and satellite navigation systems are vulnerable to attack," *Fortune Magazine*, October 15, 2001, p. 145.

Cyber terrorism can also be conducted with relative ease, low costs and a minimum amount of sophisticated technology. For instance, a computer and a connection to the Internet are all that are needed to wreak havoc from any location in the world.

On November 2, the National Infrastructure Protection Center, a branch of the FBI responsible for guarding against disruptions in critical facilities, sent out the second of two advisories warning of increased potential for computer penetrations since the attacks on the WTC and the Pentagon.

Even before September 11, 85 percent of companies surveyed in 2001 by the Computer Security Institute and the FBI reported computer breaches. Adding to these concerns is the fact that the federal government received an overall failing grade for computer security.[3] Although federal officials have promised to hold agencies more accountable, all signs seem to indicate that Internet security is at risk, and both public and private leaders must know where their weaknesses exist and take immediate corrective action.

What damage can be done?

At this point, defacement of Web sites and denial-of-service attacks have been the pinnacle of executed cyber terrorist attacks. As a result, some cynics give little credence to the actual threat posed by cyber terrorism. Yet Internet vulnerabilities can lead to substantial damages to our society as a whole.

Cyber terrorism is different from the computer viruses that harass companies on an almost daily basis in that terrorists ultimately want to utilize computer resources to intimidate, coerce others and take lives. High profile corporations may be targeted as the electronic arteries of our capitalist system, or a large network can simply be broken into and its bandwidth utilized to stage a more serious attack on the nation's critical network infrastructure.

The Center for Strategic & International Studies reports that almost all of the Fortune 500 companies' networks have been hacked into by cyber terrorists.[4] The center also reveals that it would take fewer than 30 computer hackers strategically placed around the world with a budget of less than $10 million to decimate the technological infrastructure of the U.S. economy.[5] As a result, like government agencies, the private sector must also take steps to protect itself from outside attacks.

Most experts feel that military installations, power plants, air traffic control centers, banks and telecommunications networks are at greatest risk for cyber terrorist attack. Other facilities include police, medical, fire and rescue systems, along with Wall Street financial networks, water systems, etc.

[3] "E-GOVERNMENT: Horn Gives Government Failing Grade on Computer Security," *National Journal's Technology Daily*, November 9, 2001.

[4] Lynna Goch, "Demand for Cyber-risk Policies is Growing," *BestWire*, November 8, 2001.

[5] Goch, "Demand for Cyber-risk Policies."

Here are a few examples of our nation's vulnerability:

- The GAO reported last year that the Federal Aviation Administration has "serious and pervasive problems" in the their network due to "undue exposure to intrusions and malicious attacks."[6]
- The GPS system, which the FAA wants to rely on exclusively for future airline navigation, is particularly vulnerable to "jamming."[7]
- In 1997, a teenager managed to hack into a computer servicing the Worcester, Mass. Airport, disabling an ATC tower for six hours. ATC computers remain highly vulnerable.[8]
- Earlier this year a hacker broke into the computer systems of the California Independent System Operator (Cal-ISO), the state manager of long-distance electricity transmission. There was no damage, but the intrusion made them aware of vulnerabilities.[9]
- Within days of the first U.S. air strikes Afghanistan, a group of pro-Taliban computer hackers in Pakistan penetrated several Indian government computers—including one in the atomic energy agency—and posted messages of support for Osama bin Laden and his al Qaeda terrorist network.[10]

Recession also increases risk factors

With the downturn in the economy, companies have found themselves in a quite a predicament. When corporate profits are down, one of the first areas to be cut is IT spending. Although IT professionals are not at high risk for layoffs, they may be expected to do more with less and expensive projects may be put on hold. Despite signs of decreasing financial resources, information security—usually part of the IT budget—has never been more important.

Increased layoffs can also mean increased risks. In the nine month period ending on September 30, 1.37 million job cuts have been announced, according to the outplacement firm Challenger Gray & Christmas, the highest job-cut total since researchers started tracking layoffs in 1989.

With increased downsizing, there will probably be an accompanying increase in security breaches as disgruntled employees seek revenge by sabotaging a former employer's Web site or disclosing passwords or network security information. For instance, there was a case several years ago in which a disgruntled employee left behind a logic bomb. When the computer system

6 Behar, "Fear Along the Firewall," p. 145.

7 Behar, "Fear Along the Firewall," p. 145.

8 Behar, "Fear Along the Firewall," p. 145.

9 Erik Sherman, "Terror's Next Target?" *Newsweek*, October 15, 2001, p. 68C.

10 "CYBER SECURITY: Cyberspace May Be Next War Frontier," *National Journal's Technology Daily,* November 13, 2001.

didn't see his name on payroll, it was programmed to delete files. This ended up costing the company about $10 million in damages.[11]

No computer is an island?

Making the nation's infrastructure safer is not an impossible task. The most foolproof defense against cyber terrorism is to make sure that the computers that run critical systems are not physically connected to any other computers that might be hooked up to the Internet. Removing dial-in communications —which can provide an opportunity for a system breach—can further improve security.

Richard Clarke, head of the Office of Cyberspace Security, recognizing these safety precautions, has called for the creation of an Internet-like computer network solely for government use. Unlike the Internet, this system would be entirely safe from external access.

In the meantime, government agencies and private organizations must continue to identify and secure vulnerabilities that may lead to breaches.[12]

Steps toward securing your system

Step 1: Assess your network security

Recognizing an organization's vulnerability to cyber terrorism can be truly sobering. The best antidote is a thorough and professional analysis of current systems and security, installation of software to protect networked systems from intrusion and to detect and document problems as soon as they occur.

Even with increased budget constraints, companies should keep information security a top priority. An organization may even want to step up their physical security initiatives. It is quite conceivable that although a network is secured with firewalls, encryption systems and passwords, someone could walk right off the street and sit at a computer, instantly gaining access to a company network and proprietary information.

Here are some network security issues to keep in mind:

- If your company is preparing to downsize, keep network security in mind. Many companies wait until the end of the day to notify employees. Security guards monitor employees as they collect their belongings and then escort them out of the building.
- Make sure that firewalls are properly configured to provide adequate protection. Companies should also proactively dedicate IT resources to configure network infrastructure and servers to optimize security.
- Implement, maintain and update virus detection software that includes protection at many different points of entry, including e-mail and instant messaging.

[11] Ali Velshi, "Threat of Cyber Crimes to Business," *Business Unusual*, CNNfn, Transcript #110104cb.112, November 1, 2001.

[12] Stefanie Scott, "Hackers Seek to Disrupt Production, Profitability, Say Wisconsin Analysts," *The Post Crescent*, October 29, 2001.

- Make sure that vendors, partners and contractors have signed confidentiality contracts regarding proprietary information and are trained on how to keep this information from getting into the wrong hands.
- Establish computer networking and Internet policies so employees are aware of risks they may expose the company to. For instance, downloads of games and software can expose the company to "Trojan horse" applications, viruses, worms and other types of security breaches. As a result, all software installations and downloads should be limited or at least cleared through an information security specialist.
- Have a designated information security specialist in your IT department. Keeping up with the latest viruses, exposures and risks is a time consuming function. Even if you outsource information security to another company, there should be one point of contact at your company to ensure that all tasks are being done to keep firewalls, virus protection and policies up-to-date.

Step 2: Assess your cyber risks and policy coverages. E-business insurance policies can assist in covering losses due to both first party damage and third party liability resulting from cyber activity. Traditional business insurance may not cover cyber intrusions and e-business liabilities. These policies were written long before the Internet, electronic communication or e-commerce, and usually focus on very tangible, real-world property damage.

Here are some questions to ask when assessing your coverage needs:

- Are you covered by a traditional carrier?
- Does your policy exclude digital data as property? In other words, are first-party damages due to a virus or security breach covered in the policy?
- Will your policy cover cyber terrorism?
- Is your company involved with new media publishing that might expose it to third party liability issues? For instance, does your company publish a Web site or an e-mail newsletter?
- Should your organization consider a third party liability policy due to customer privacy concerns?

Step 3: Be particularly aware of policy exclusions.
To be thorough, a company should carefully examine definitions, limitations and special clauses in their existing coverage to identify potential gaps and exposures, and the potential financial losses from these exposures.

With experts claiming that cyber terrorism may be the next weapon used against the United States, some insurers and underwriters are stepping up to offer specialized coverage for this new risk. On the other hand, some insurers have anticipated that huge losses could potentially arise if simultaneous attacks occurred in millions of companies across the country, and have

actually clarified their property policies to say they do not consider software and databases to be “property.”

The problem is primarily one of definition, in which “property” with most insurers is defined in a physical sense. Using this explanation, insurers would only cover business interruptions due to physical damage caused by fire or water, for example. This leaves companies to purchase separate coverage for losses caused by computer viruses, hackers and security breaches.

Step 4: Utilized specialized underwriting services.
When looking for appropriate coverage, utilize an IT security expert and a managing general underwriter that specializes in e-business risks. Cyber risks and network security have unique loss exposures that require specialized new insurance products and risk management. A specialized carrier or managing general underwriter can help companies determine the types of coverage and specialized insurance products they need for their particular e-risks.

For some companies, the cost of business interruptions and repairing systems may be insignificant in comparison to the liabilities they would face if client privacy were invaded. In this case, they should consider a third-party liability policy to cover damages done to another party as a result of the their e-business activities.

The future of network security

As corporate purse strings tighten, IT staff may be pressured to keep systems running with less resources, with important security maintenance—such as updating virus protection software or installing network system patches—falling by the wayside. This can leave an opportunity for lurking hackers to sneak in the backdoor. As a result, public and private leaders must continue to hold information security as a top priority. While no one can be completely immune to cyber attacks in this day and age, those who are well prepared will sleep better, and suffer less damage should an attack occur.

Philip Pierson is founder and manager of e-Sher Underwriting Managers, a company that works in conjunction with leading edge security assurance developers, counselors and intelligence experts to provide policyholders with high quality risk and security assessments and products, to avoid or at least mitigate damage to computer networks and information assets before they occur. For more information, visit **www.e-sher.net** or contact Mr. Pierson at **philip_pierson@swett.com,** 949-477-6646.