PROSKAUER ROSE®

Client Alert

A report
for clients
and friends
of the firm

November 2002

Business Computers and Networks Are Vulnerable to Infiltration

Cyberattacks a Real Threat in the Post-9/11 World: Tips on How to Be Prepared and How to Reduce Legal Risk

The headline in a late-January, 2002 *Washington Post* read "Computer attacks on companies up sharply. Systems vulnerable to cyber strikes". The accompanying article confirmed what had been feared after September 11: terrorists and cyber-criminals are lurking in cyber-space and threaten real harm to businesses from cyber-attacks.

Expecting the unexpected has become a way of life. And for businesses unprepared to deal with cyber-attacks, the risks to ongoing operations and the legal risks are substantial.

A cyber-attack is an invasion intended to compromise a computer or network. There are many forms of cyber-attacks — denial of service attacks, flood attacks, logic bomb attacks, Web Site defacement, virus attacks and theft of proprietary information — all having the power to inflict enormous damage, if not irreparable harm, to businesses.

Gone are the days when attacks into network systems were dismissed as random acts of idle, computer-savvy teenagers. Rather, cyber-attacks and cyber-terrorism have joined hijacking and biological attacks on the list of threats that businesses must be prepared to face. The prevention of such cyber-attacks has, therefore, become an obligation of doing business. Understanding such risks can help companies develop an effective survival plan that addresses both business continuity and disaster recovery. In addition, a business that plans to prevent and deal with computer intrusions will be in a better position to resist legal liability.

As businesses prepare to combat cyber-attacks, they will need a three-part strategy: (1) prevention and prophylactic measures; (2) containment once an attack takes place; and (3) remediation in getting a business back on its feet.

Prevention and Prophylactic Measures to Reduce the Risk of Cyber-Attacks

In the process of setting up shields against cyber-attacks, risk recognition is key. Attack prevention can be achieved through a variety of techniques.

1. Conduct Network Assessments

   The most crucial step in risk recognition involves vulnerability assessments and penetration testing. Prudent companies orchestrate mock break-ins into their networks to evaluate how vulnerable the company is to hacking and other attacks. Although network security audits may be conducted by internal personnel, companies should consider hiring an outside security consulting firm to maximize objectivity and avoid the risk that internal staff may be too close to the issue. By conducting a business impact assessment, companies can test the strength of the plan and ability to make a timely response. The consultants can also assist with the development of a recovery plan, the implementation and testing of the plan and the maintenance and quality control of the procedures.

   Vulnerability testing may be a costly initiative for many companies. The alternative of leaving a business open to a cyber-attack, however, may inflict costs that threaten the very survival of a business. These risks include irreparable damage to network systems, company liability for the failure to take reasonable steps to protect the business from cyber-attacks in the form of shareholder or customer suits, or a challenge launched by insurers, and damage to a company's reputation and good name.

2. Firewalls, Passwords and Other Security Measures

   Attack prevention can be achieved through a variety of means. The creation of firewalls and guards have become a "must do" for virtually every business having an online presence. Firewalls act like checkpoints, requiring all traffic passing through, whether inside or outside, to request permission. If proper authorization is not granted, the firewall

will either block the traffic or channel it to specific designated areas until express authorization is provided. Firewalls must be checked and updated regularly.

Companies also should take steps to preserve the integrity and confidentiality of their businesses by establishing password protection systems that are impervious to invasions. A recent report by the Federal Bureau of Investigation revealed that fifty-five percent of survey respondents reported threatening activity by *insiders*, making insiders a formidable threat to cyber-security.[1] Consider the scenario of a former disgruntled employee, who created a "backdoor" for himself into a system. Using the backdoor, the former employee obtains system administrator passwords and sensitive program files maintained on the internal network, crashes network servers and erases all of the server volume on each of the crashed servers. For no more than a few hours of work, such an intrusion may result in millions of dollars in damages and force a company to shut down operations. An obvious way to prevent these types of attacks from occurring is to terminate network access as soon as a decision is made to terminate an employee.

Companies should also consider the following measures to better safeguard their systems: (1) implementing boundary controls with security policies; (2) monitoring, on a constant basis, the computer network; (3) frequently updating the software to make certain that all current patches and bug fixes have been installed; (4) storing system information on back-up tapes and making certain that a back-up server could be in place at an off-site location; (5) using encryption to encode certain types of communications such as e-mails; (6) loading anti-virus software; (7) maintaining proper insurance coverage for cyber-attacks and taking steps specified in the policy to secure the company's system; and (8) establishing emergency responses or counter-measure plans in the event of a cyber-attack and periodically updating these plans.

Containment and Emergency Responses in the Event of a Cyber-Attack

1. Deciding Whether to Shut Systems Down
In the event of a cyber-attack, what happens and how fast it happens are crucial. Business continuity, or dealing with the immediate response of locating employees and determining the necessary steps to start up computer systems and networks again, becomes top priority. After a cyber-attack, however, a company is faced with the difficult dilemma of deciding whether to shut systems down — and risk losing the trail of electronic footprints — or keeping its ports open and risking that the perpetrator will gain re-entry into the system and cause more damage. Without preserving the means to trace the attacker's activities, there are no means to establish accountability. In many cases, the simple act of re-booting a computer in an effort to expunge the system of the program installed by the hacker can destroy valuable evidence. Such determinations, therefore, turn upon the individual facts surrounding a particular attack. In cases where the attack has lead to a theft of trade secrets, customer-related data or other sensitive, proprietary information, the decision to leave ports open could invite another invasion to take place and increase damages. The failure to shut down a system could also result in the loss of trade secret protection if a court were to find that a company did not take steps to protect its proprietary information by securing its systems once it had reason to suspect a breach. If, however, the attack resulted in merely a web site being defaced, it may be less dangerous to leave the system open in hopes to trace back the electronic footprints of the attacker.

2. Determining Whether the Attack has Ceased
Once there is reason to believe a cyber-attack has taken place, a company must determine whether the attack has ceased. The initial response, therefore, includes controlling the attack from a technical standpoint. In this regard, the internal IT department should make sure that the affected systems have been shut down or isolated to perform an analysis of the problem, locate the vulnerability and protect other areas of the network. The IT staff may also consider taking pictures of program files, which can later be given to law enforcement or used in internal investigatory functions. As already stated, these tasks must be balanced with the need to preserve evidence that may be later used in a lawsuit or criminal prosecution.

3. Notifying Appropriate Company Employees
Companies should create a list of individuals to contact in the event of a cyber-attack. The list should include people such as senior-level executives in charge of IT (*i.e.*, Chief Information Officer), the IT director and the security director. Other people to notify include a contact person in public relations to assist in creating a press release, monitoring all news on the attack and formulating a proper media response on behalf of the company, and the general counsel and/or outside counsel to develop a legal strategy in preparing a lawsuit, discovering the identity of the attacker, contacting insurance companies and making referrals to appropriate law enforcement authority. In addition to contacting key employees *within* the business, companies may also consider hiring an outside third party computer security or forensics company to evaluate and monitor the computer network.

4. Deciding Whether Law Enforcement Should be Contacted
Companies should assess whether to bring in outside law enforcement powers in containing an intrusion that compromises network security. Unlawful intrusion into a computer network, theft of proprietary data or destruction of files is a crime, where there are both state and federal legal

[1] *See* Congressional Statement, Federal Bureau of Investigation, National Infrastructure Protection Center Cyber Threat Assessment, Oct. 1999, Before the Subcomm. on Technology and Terrorism of the Senate Comm. on the Judiciary (Oct. 6, 1999).

remedies. Companies may consider resorting to law enforcement where the amount of the actual loss exceeds a certain amount (*i.e.*, $100,000), customer data or trade secrets have been stolen, national security interests are implicated by a terrorist threat from the attack, the attack affected multiple computer networks or the company is one of the nation's infrastructure companies. In certain cases, the nature of the cyber-attack (*i.e.*, national security threat) may create an obligation for a business to notify government authorities.

Although the government enjoys a monopoly over criminal law enforcement, companies, nonetheless, may have a choice in selecting which law enforcement entity to contact. As such, the Federal Bureau of Investigation, United States Secret Service, the Federal Trade Commission or the state attorney general's office may be contacted. Handing the matter to law enforcement, however, presents potential conflicts between the goals of a private company and the government, where a company's focus will likely be on remediation and business continuity, and the government's focus will be on investigation and bringing the perpetrator to justice.

Remediation and Establishing Accountability for the Attack

Once the attack has been isolated and a company has its arms around the problem, it must transition into disaster recovery mode in dealing with the actual information technology side of storage, back-up and network solutions. As well, determining the identity of the attacker will be a key priority as the company attempts to remediate and safeguard against future intrusions.

1. Determining the Identity of the Attacker

   There are a variety of legal routes available to companies attempting to discover the identity of the attacker. One way is to file a "John Doe" lawsuit, where an unidentified litigant is named as the defendant. Once the lawsuit is filed, the plaintiff-company may seek discovery in efforts to determine the identity of the attacker. Although John Doe actions entitle a plaintiff to all the powers offered through discovery, filing a formal lawsuit may subject the plaintiff to extended time lags between filing and discovery and, therefore, may not be a viable option for many companies.

   Subpoena powers may also be used in compelling an Internet Service Provider ("ISP") to disclose the name of an Internet user, but the aggrieved party often must make a showing of entitlement before a court will order the disclosure. Certain states allow a party to seek limited discovery from an ISP, through court order, without the filing of a full-blown lawsuit. In obtaining such an order, however, the aggrieved party must set forth a variety of factors, which may include showing: (1) that it seeks the information in good faith; (2) the information relates to a core claim or defense in the action; (3) the identification is directly and materially relevant to a core claim or defense in the action; and (4) information sufficient to establish or rebut the core claim or defense is unavailable for any other source. This limited discovery proceeding, however, may invite ISPs to challenge or even file counterclaims in response to disclosure requests.

2. Filing an Action Once the Identity of the Attacker is Discovered

   Companies contemplating filing an action to collect damages from a cyber-attack may look to several federal and state statutes, including the Computer Fraud and Abuse Act ("CFAA"), the Electronic Communications Privacy Act ("ECPA") and state unfair and deceptive trade practices statutes. Moreover, it may be prudent for companies to file a lawsuit in a favorable forum in preempting a potential shareholder derivative lawsuit for failure to implement appropriate security safeguards, act within the parameters of the business judgment rule or seek damages from the attacker.

   The CFAA is the principal federal statute that addresses most of the ways in which computers may be attacked as the object of a crime, prohibiting unauthorized access to not only computers that belong to the government and financial institutions, but any computer that is used in interstate or foreign commerce. The CFAA proscribes a wide range of conduct including access that is used to obtain national security information or financial records, intercept interstate communications, manipulate government computers, defraud and obtain anything of value worth $5,000 or more, traffic in passwords, or extort by threatening to damage a computer. The statute also provides a private right of action so long as damages exceed $5,000, allowing a plaintiff to recover actual economic damages and equitable relief. A company contemplating filing an action under the CFAA should, therefore, assign a dollar value to its damages, including the information that was stolen as well as the cost to identify and repair.

   Under the CFAA, employees who exceed their authorized use and intentionally causes damage are just as liable as an outside hacker who intentionally broke into a system. Damages caused by authorized people and company insiders who were reckless or negligent, however, are not criminally culpable under the CFAA. As applied to outside hackers, however, the CFAA does not draw such a distinction and criminalizes the hacker for damages arising from the attack, whether it was negligent, reckless or intentional.

   The Electronic Communications Privacy Act ("ECPA") protects against unlawful interceptions of communications, including e-mail and other data sent over wires and prohibits the unauthorized access of stored electronic communications. There is, however, a provider exception for companies that provide e-mail or voicemail services for its employees on its own computer system. The ECPA also provides a private right of action for a company that had its communications intercepted or illicitly accessed, and plain-

tiff may recover actual and punitive damages, equitable relief and attorneys' fees.

Advisability of a Legal Audit

Obviously, the main objective for a business dealing with potential or actual cyber-attacks is prevention and business continuity. A secondary, but important, objective is insuring that the legal risks are minimized. This can be accomplished through a legal audit that works in tandem with the technological audit.

A legal audit of a company addressing cyber-attacks should include, at a minimum:

1. A review of all applicable insurance policies and coordination with the risk management personnel and insurance brokers;
2. A review of the documented steps in place to prevent cyber-attacks;
3. A review of public statements, including securities filings, regarding the level of security in place and what contingency planning exists;
4. A review of emergency preparedness manuals and communications plans;
5. A review of precautions against the theft of proprietary and confidential business information of the company and its clients; and
6. A review of applicable privacy policies and their intersection with security measures.

A legal review to insure that the company has acted reasonably to deal with cyber-attacks, documented its actions, disclosed its readiness honestly and obtained indemnification, where possible, should be part of any preparedness plan.

Has Your Address Changed?

Please let us know if your mailing address needs to be updated. Contact Deborah Chernoff with the correct information either via e-mail: dchernoff@proskauer.com or fax: 212.969.2900.

You can also visit our Website at **www.proskauer.com**

Conclusion

Cyber-attacks have evolved from once being simple teenage pranks to becoming sophisticated threats that have the potential to cause severe economic damage to a company, if not its collapse. Businesses must be prepared for the real threat of falling victim to a cyber-attack. Companies should, therefore, develop and administer a comprehensive security plan and consider their options in making their systems cyber-attack proof. Then, working with counsel, the company should work to reduce its legal risks to the extent possible in these uncertain times.

NEW YORK LOS ANGELES
WASHINGTON BOCA RATON
NEWARK PARIS

Client Alert

For further information on technology law issues, please contact:

Christopher Wolf
202.416.6818 - cwolf@proskauer.com

Scott Cooper
310.284.5669 - scooper@proskauer.com

Hank Goldsmith
212.969.3418 - hgoldsmith@proskauer.com

1585 Broadway
New York, NY 10036-8299
212.969.3000

68, rue du Faubourg Saint-Honore
75008 Paris, France
331.53.05.60.00

2049 Century Park East
32nd Floor
Los Angeles, CA 90067-3206
310.557.2900

1233 Twentieth Street, NW
Suite 800
Washington, DC 20036-2396
202.416.6800

One Newark Center
18th Floor
Newark, NJ 07102
973.274.3200

One Boca Place
Suite 340 West
2255 Glades Road
Boca Raton, FL 33431-7383
561.241.7400