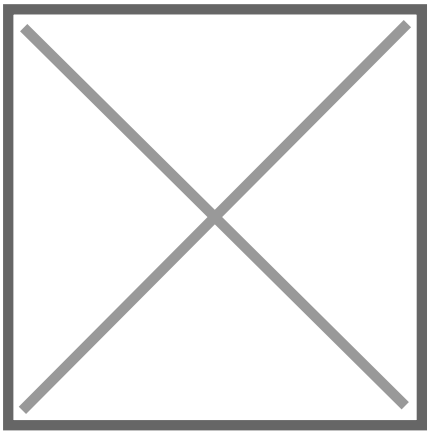
WIGGIN

WIGGIN AND DANA



Computer Intrusions: A Company's Options When Its Systems Have Been Hacked

Introduction

The explosive expansion of the Internet and e-commerce has transformed business and the global economy, creating unparalleled opportunities for increased productivity and economic growth. Nearly every company has adopted an "e-strategy," exploiting the connectivity of the Internet to manage more successfully their relationships with employees, customers and business partners. The proliferation and ubiquity of e-mail, corporate intranets, online databases and other web-based information technologies have created a powerful digital infrastructure, which has in turn enabled worldwide access to and retrieval of critical information and corporate resources.

Unfortunately, the convenience and efficiency of the Internet have come at a price. The same technologies that connect and empower corporations can expose their vital proprietary information to unwanted discovery and revelation, presenting alluring and sometimes irresistible opportunities for unscrupulous competitors, disgruntled employees or malicious snoops.

Incidents of computer intrusion and other cyber-crimes have increased exponentially over the past decade and promise to escalate further as the Internet becomes more thoroughly entwined in economic life. The FBI opened 547 new computer intrusion cases in 1998 and 1154 new cases in 1999, and the number is expected to have risen dramatically in 2000. The Computer Security Institute's 2001 Computer Crime and Security Survey determined that computer security breaches cost U.S. companies over $377 million in 2000. In that survey, 85 of respondents reported computer security breaches within the prior twelve months, 70 identified the Internet as a point of attack by

outsiders, 49 reported attacks by insiders, and 58 of those reporting unauthorized access reported ten or more hacker incidents.

Facing these formidable challenges, responsible companies are devoting corporate attention and resources to the creation and maintenance of effective information security regimes. Nevertheless, each technological security innovation contains in its inception the seeds of new circumvention, making it difficult for even the most vigilant company to avoid the damaging impact of a major computer intrusion.

This article will explore the best options available to a company that suffers a successful hacker attack. The article will first outline the principal federal statutes related to computer hacking. It will then describe the principal courses of action available to a corporation, highlighting the primary advantages and disadvantages of each approach.

Pertinent Statutes

Three principle federal statutes prohibit computer hacking and other unauthorized uses of computers and computerized information: the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act and the Economic Espionage Act. While none addresses completely the full range of computer crimes, most cyber-crimes fall within the scope of one or all of these laws.

The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA) criminalizes certain fraudulent activities related to computers and electronic records and is the primary criminal statute related to cyber-crime. The CFAA focuses on security (the protection of computers and computer networks), rather than on the privacy of digital information. Particular information is protected only as a byproduct of the protection afforded the physical computer in which the information is stored.

The CFAA contains seven separate criminal offenses and is directly implicated by the activities of most computer hackers and cyber-criminals. Generally, the CFAA prohibits the unauthorized access to or damage of a “protected computer.” The term “protected computer” is defined broadly as a computer “exclusively for the use of a financial institution or the United States Government . . . or which is used in interstate or foreign commerce or communication.” The statute protects any computer connected to an interstate network, such as the world wide web. For purposes of the statute, a person “exceeds authorized access” by “access[ing] a computer without authorization and us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.”

The CFAA specifically prohibits obtaining anything of value by accessing a protected computer without authorization or, in accessing such a computer without authorization, causing damage, which includes:

> any impairment to the integrity or availability of data, a program, a system, or information that (a) causes loss aggregating at lease $5,000 in value during any 1-year period to one or more individuals; (b) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals; (c) causes physical injury to any person; or (d) threatens public health or safety.

The CFAA authorizes the imposition of significant fines and lengthy imprisonment. The CFAA also authorizes civil causes of action to obtain compensatory damages and injunctive relief.

The Electronic Communications Privacy Act

The second federal statute applicable to a hacker attack is the Electronic Communications Privacy Act (ECPA). Enacted in 1986, the ECPA was Congress' effort to apply existing privacy laws to electronic communications transmitted through new technologies and electronic media. Congress extended the privacy protection then afforded telephone networks under the 1968 Wiretap Statute to new forms of electronic records and digital communications, such as electronic mail and voice mail messages.

In general, the ECPA prohibits unauthorized access to electronic communications intended as confidential. The stored communication provisions of the ECPA specifically prohibit unauthorized access to or use of stored electronic communications. This unauthorized access applies both to external hackers and to authorized internal users who exceed their authorization. Significantly, the unauthorized access is itself a crime; there need be no further conduct. The statute also prohibits operators of electronic communication services from disclosing stored communications, unless such disclosure is (i) authorized by the sender or recipient of the message, (ii) to an intended recipient of the message, (iii) necessary for the efficient operation of the communications system, or (iv) required by the government.

The ECPA authorizes the imposition of significant criminal penalties, including imprisonment. Additionally, an aggrieved party may bring a civil cause of action for any "knowing or intentional" violation of the ECPA and may recover monetary damages, including actual damages, attorneys' fees and "any profits made by the violator as a result of the violation." Accordingly, the ECPA provides a powerful statutory weapon against the activities of computer hackers and cyber-criminals.

The Economic Espionage Act

The third and final federal statute often triggered by a hacker attack is the Economic Espionage Act (EEA), which criminalizes the theft of trade secrets and other proprietary information. The EEA embraces an expansive definition of the term "trade secret," sweeping in:

> all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by the public.

The statute imposes substantial monetary and criminal penalties for violations, with the severity of the penalty turning on the identity of the violator. Importantly, however, the EEA is exclusively criminal, imposing no civil liability to the trade secret owner, except for injunctive relief.

A Company's Primary Options

Proper planning and prevention is still the best defense against the threats posed by hackers and other cyber-criminals. Most cyber attacks exploit known, and often easily fixed, security flaws in browsers, operating systems and other software. Promptly addressing already-identified security problems throughout a company's corporate network is therefore the simplest, cheapest and most effective strategy for reducing the risk of suffering a successful hacker attack.

Nevertheless, the protection that can be gained from technology and planning is necessarily limited. For example, many hackers do not focus on technology when looking for weaknesses in a particular computer network. Rather, a practice known as "social engineering" — manipulating employees or other authorized users to disclose passwords or other confidential information — is a favorite method for gaining access to a company's computers. This practice is difficult, if not impossible, to stop using technological solutions.

Moreover, computer technology is speeding along at a break-neck developmental pace, and the rush to market for new technologies often overwhelms security concerns. Each new product contains new security weaknesses, which are quickly exploited by hackers, and even as some known flaws are repaired, hackers uncover others with impressive ingenuity and alacrity. This dynamic of computer security management inherently limits a company's ability to protect itself from all forms of computer intrusion, and every company therefore must prepare strategies for responding to the economic impact and corporate after-shocks of a successful hacker attack.

The principal options available to a corporation following a breach of its computer security can be divided into three basic categories: (1) pursuing self-help remedies; (2) referring the case to law enforcement authorities; and (3)

bringing a civil action. Each option has decided benefits and detriments, including expenses, timing, limitations on remedies, and public relations effects.

1. Self-Help

One possible course of action available to a victimized company is to choose not to disclose to third parties news of the attack and simply improve the company's internal computer security. Companies are often fearful of publicizing a successful attack on their systems, concerned that the news will shake investor confidence or undermine their competitive position in the marketplace. Corporate managers also worry about the potential impact of involving law enforcement officials, imagining scores of FBI agents combing through their computer systems and confiscating hard drives and sensitive data. Thus, when faced with the problem, some companies find the self-help path appealing.

This option, however, is quite problematic. First, the success of the initial attack should cause the company to doubt the reliability of computer security systems as an exclusive approach to the prevention of cyber-crime. Additionally, it is extremely unlikely that the company could actually keep the attack secret, so any effort to hide an attack could seriously damage the company's credibility. While improving computer security is always desirable, public denial of a computer attack will likely fail and may exaggerate public perceptions of the incident and the damage it caused.

The Internet is a powerful communicative tool, and hackers often boast about their accomplishments in cyberspace, publicizing rather than keeping secret a major attack on a company's corporate computer systems. The larger the violated entity and the more extensive the violation, the more likely that news of the incident will rapidly spread throughout the Internet community. Official denial in the face of proliferating Internet rumors can lead not only to a widely held belief that the attack actually occurred but also to a general perception that the company is not taking steps to address its computer security problems. The latter perception will inevitably have a longer lasting and far more devastating effect on a company's bottom line than an honest public admission about a recent hacker attack. This is particularly true when the admission is coupled with an announcement regarding the security measures the company is putting in place to protect itself from future harm. A well-publicized, company-wide security audit performed by a nationally recognized computer security firm, even one conducted on the heels of a successful hacker intrusion, demonstrates an important corporate awareness of computer security issues and can help generate renewed confidence from customers, suppliers, and investors.

Prompt reporting of hacker activity and publicizing particular security flaws also produces important positive social benefits. As mentioned above, most computer attacks exploit known security flaws. Keeping secret a computer intrusion prevents law enforcement and software vendors from quickly uncovering and responding to new security problems, ensuring the success of similar repeated attacks. Hackers often use the communicative power of the Internet to share information, and savvy companies can use this same tool to expose hackers and thwart future cyber-crimes by diligently investigating and publicizing incidents of computer intrusions.

Also, a failure to implement widely available computer security systems might subject the company to potential liability from its clients or shareholders, if the company is attacked by a hacker who would have been thwarted by such reasonable precautions. Officers and directors owe fiduciary duties of care to their companies, and a court might view a disregard for basic computer security issues as a breach of that duty. Clients of a victimized company who have their information damaged or stolen could argue that the company acted negligently in failing to address known computer security risks. Additionally, companies often have contractual duties to protect the security of client information, the abrogation of which might expose the company to a breach of contract claim from an affected client.

2. Civil Litigation

Bringing a civil lawsuit offers a company the only method for recovering full monetary damages (beyond restitution) from the violator. As discussed above, several federal statutes authorize the imposition of heavy financial penalties and permit the recovery of actual and punitive damages. Accordingly, a civillaw suit can be an appealing response to an intrusion by a competitor or other entity with substantial financial assets. It may not, however, suit the criminal activities of a lone computer hacker with few economic resources and little ability to pay a significant legal judgment.

Moreover, mounting an effective civil lawsuit requires quick action and substantial expenditures of corporate time and treasure. A company must retain experienced legal counsel and hire computer experts to collect and preserve the evidence for trial. The detective work involved in uncovering the identity of the intruder is beyond the skill and resources of many companies, and even if a company can identify the source of the attack, the complexity of the technology involved can make proving the case in court very difficult. Thus, the preparation for trial and the trial itself are necessarily time-consuming and expensive, offering little chance for an immediate resolution.

A civil lawsuit also means that the company must formally and publicly acknowledge the hacker's activities and success, identifying the scope of the attack and the type of information compromised. This often involves a public admission that sensitive, proprietary corporate data was disclosed to third parties or, still worse, published on the Internet. This public aspect can often discourage civil enforcement or even the reporting of computer crimes. Large financial institutions, for example, generally resist openly acknowledging that their customers' accounts or other financial records were accessed illegally. E-merchants, already facing wary and distrustful consumers reluctant to provide payment information over the Internet, are often unwilling to admit publicly that confidential customer information was stolen in a hacker attack.

Nevertheless, depending on the scope of the violation and the resources of the violator, the full scope of economic and injunctive relief available through a civil action can provide a compelling justification for selecting this option. For example, in a corporate espionage case — where a competitor illegally accesses trade secret information or other proprietary data – actual and punitive damages may be the only sufficient remedy or may at least offer the only substantive compensation for the damage caused. This is particularly true if the hacker discloses the stolen trade secret information and thus places what was valuable proprietary knowledge into the public domain.

Finally, a civil suit offers companies a great deal of control over any investigation and flexibility throughout any subsequent trial. This control can mean the difference between keeping private sensitive or embarrassing information and being forced to publicly disclose such information as part of an official government investigation. Controlling the process also allows a company the flexibility to negotiate a favorable settlement, even if such a settlement would not be the socially optimal outcome. Any legal action by law enforcement officials would necessarily be motivated and constrained by the public interest. A company engaged in a civil lawsuit is free to pursue its own goals, despite any overarching government concerns. For all of these reasons, civil litigation may be the best available option and should be considered seriously by any corporate hacking victim.

3. Criminal Referral

The victim of a hacker attack may also refer the case to federal or state law enforcement officials. This option offers companies a low-cost avenue for pursuing cyber-criminals, while still presenting a positive public image as a responsible corporate citizen. Unlike a civil lawsuit, government action is financed by the taxpayers, presenting an economically efficient method for responding to malicious computer intrusions. Start-up companies with thin legal budgets, for instance, can use law enforcement as an effective tool for avoiding expensive civil litigation while still taking responsible steps to respond to hacker attacks and other cyber-crimes.

As mentioned above, however, the savings in money comes at the price of control, so companies should carefully weigh this trade-off before deciding upon a course of action. Once the case is turned over to law enforcement, the government obtains access to the victimized company's facilities and computer files, the government controls the process and pace of the legal investigation, and the government, not the company, decides what evidence is disclosed at trial. The government also determines when and whether to resolve the case, which can lead to unwanted consequences for the company.

In contrast to a civil lawsuit, a criminal investigation will not bring a victim punitive damages, only financial restitution, so a successful prosecution by law enforcement may not afford an equal remedy. For example, a denial of service attack on a major e-commerce website might shut the site down for hours or even days, generating ill-will from customers who cannot access the site and resulting in significant financial losses. The owner of the site is unlikely to recover those intangible losses through a criminal investigation.

The government is usually far better equipped to track down cyber-criminals, most of whom roam the Internet with pseudonyms. A federal grand jury has almost limitless power to probe a competitor's practices, conducting interrogations of employees and demanding production of all but privileged information, and the grand jury's greater powers may make the difference between a successful and an unsuccessful litigation. The government has also made it clear that it appreciates the risk of inadvertently disclosing proprietary company information during the course of a criminal investigation and that it will work with companies to minimize the risks of such unwanted disclosures.

Furthermore, law enforcement officials realize that they need corporate cooperation and trust to combat effectively the myriad criminal threats enabled by the net and are increasingly adapting their investigative practices accordingly. For example, criminal investigators rarely need to confiscate computer hard drives or disrupt computer networks. Rather, they can mirror effected drives and can often gather evidence remotely during off-peak hours. Similarly, criminal investigations often occur discretely, with the first public statement regarding the attack occurring at the press conference announcing the arrest of the suspected perpetrator. Government involvement, therefore, should not itself dissuade a company from turning a hacker case over to law enforcement officials.

Finally, government action is often the most effective and desirable response to intrusions by insiders or rogue hackers. These perpetrators will not likely have the money to pay large civil judgments, and high-profile investigations of this type of cyber-crime and the publicity surrounding its punishment can deter future attacks. A civil suit brought by a company against an employee, even if that employee illegally accessed confidential files or somehow damaged the company's computer systems, can also have a negative impact on the attitudes of the company's other employees. Prompt action by law enforcement allows the company to protect the security of its proprietary information while, to a large extent, divorcing the company from the legal proceedings against the employee. This distance can help the company balance its need to respond firmly to insider hacking with its desire to maintain morale among its existing employees.

Conclusion

Companies should respond to a computer intrusion with a balance of prevention and prosecution. The legal response to a hacker attack can take several forms, requiring the company to weigh many factors before selecting a course of action, but legal action, in some form, is almost always better than trying to suppress the news of the attack. While no amount of computer security planning can guarantee a company that it will be free from computer hackers, proper planning can certainly shift the probabilities in the company's favor.

This article republished with permission from law.com.