



Facing Down Computer Security Threats

Being knowledgeable about technology is now part of the job.

Aside from this rule change, general counsel must now also become knowledgeable and aware of computer security threats and how these threats can harm their company, and take steps to eliminate or, at least, minimize the risk and harm.

This article will discuss current computer threats and what general counsel need to start doing to prepare for today's computer security risks.

Learning the Ropes

If you choose not to become engaged, the risk to your company is enormous. Consider that computer network systems have become the lifeblood of the average company. Manufacturers use computer network systems to run assembly lines and create products. Suppose that a computer incident disables your assembly line for days. Can your company survive such an event? Today's new phone systems are operated through computer networks. Suppose that your phone systems crash because of an attack. What if credit card information is stolen from your company's mainframe? What if the company that has a significant portion of its sales generated through the Internet learns the Web site is shut down? The list goes on.

The point is that your company, exposed to threats on a daily basis, needs to approach the issue from at least three distinct perspectives: 1) companies have to make reasonable attempts to prevent computer security intrusions; 2) companies have to be prepared to deal with computer security intrusions, not if, but when it occurs; and 3) general counsel have to make decisions regarding both these responsibilities with the goal of defending their companies from potential lawsuits grounded in common law negligence, privacy rights, and other commercial litigation. Are you doing enough to ward off litigation?

- What kind of threats do your companies face? According to Keith Jones, a computer forensics expert for the D.C.-based firm of Jones, Rose, Dykstra and Associates, all companies face threats from two primary sources—external and internal. According to Mr. Jones, the most devastating threat to a company comes from an internal attack. Why? Because insiders typically have two components critical to a successful attack, namely, 1) the ability to bypass security with ease, and 2) intimate knowledge of a company's business and network architecture. This combination can be

lethal. (See *United States v. Roger Duronio*, Crim. No. 03-933, (D. N.J.). Retail brokerage company's system administrator in 2002 unleashed "logic bomb" on company's system. An appeal of the defendant's conviction for securities fraud and computer intrusion is currently pending. The author was lead prosecutor in the case.)

According to Mr. Jones, most of today's external threats come in two main forms: 1) malicious e-mail—an e-mail containing a tool or exploit that allows the attacker access to the victim's computer system; and 2) malicious Web sites—a Web site containing a tool or exploit that allows an attacker access to the victim's computer system. The goal of today's hackers is financial gain. Stealing valuable personal data, like credit card information or financial account information, is in vogue right now. Today's hackers are driven by a motive to make money. Think of it as virtual bank robbery.

- Learn about your company's network architecture. The starting point for any general counsel is to obtain a basic understanding of the company's network architecture. This basically means understanding how the company's computer networks are used and connected to each other. Why is this important? Because understanding how the systems are connected will assist you in understanding the vulnerabilities of the computer network systems.

Does the network architecture rely upon one central computer, like a mainframe computer, or does the network architecture consist of servers, or perhaps a combination of both? What operating system(s) does the company employ? What critical network systems control the key operations of your company? At this stage, your function is to gain a basic understanding of how the systems work and are connected and begin the process of interacting with the network architecture experts in your company.

- Understand the roles of all the participants in your company's computer network systems. Of critical importance is understanding the different groups that are involved with the various computer network systems, the groups' respective functions and how they relate to each other. Most lawyers understand that if you have a problem with your laptop, contact the computer guy or gal in the office. However, within many companies with

BY MAURO M. WOLFE

EVERY DAY companies face computer threats that could have a devastating effect on business. On a daily basis, computer security incidents are reported in the news. On the front line to protect companies are lawyers who through no fault of their own are not equipped or trained to guide their companies through the murky waters ahead. The lack of education and training to easily assimilate other non-legal, technical disciplines is the issue.

The speed at which business technology changes is staggering, and the attorneys who service business clients must ready themselves to keep up with the constant change. In short, the skill necessary for lawyers to thrive in the new millennium is to understand technology, period. For the sophisticated general counsel the subject of computer technology is no longer an elective. For instance, in the past several months, the Federal Rules of Civil Procedure have forever been altered so that litigators and general counsel must now be aware of where computer data resides, on what computer network systems the data is stored, in what format the data is stored, and how to preserve the data.

Mauro M. Wolfe is a partner in the New York office of Dickstein Shapiro and formerly an assistant U.S. attorney in the District of New Jersey where he was lead prosecutor on the Duronio case, mentioned in this article.

large computer network systems, there may be a series of groups, or fiefdoms, that the attorney must deal with in order to gain a full understanding of the computer network system. For instance, in some companies, there is an IT department that has under its umbrella numerous participants with distinct, and often competing, roles: system engineers whose job it is to fix the hardware, or system administrators, software engineers, computer techs, or computer security, password security, and physical security experts. Navigating among these groups and listening to their concerns and advice is an important skill.

- Learn about your company's computer security vulnerabilities. In most large companies, the IT department routinely conducts internal and external computer security assessments or audits. Reports describing the findings of these assessments or audits are prepared, often describing in great detail the areas of concern. These reports are invaluable for attorneys in the process of understanding potential litigation risks. In most instances, the reports would be discoverable and often contain information that would be useful to plaintiffs and/or regulators, or law enforcement, particularly when the reports describe security weaknesses that were the cause or potential cause of the recent harm.

General counsel would be wise to review the reports with the IT experts within the company and with outside experts to evaluate the risks, identify a plan of remediation, and follow up. The worst thing that could happen for a company is to identify the risks and do nothing. Document the remediation.

After learning about your company's computer network systems, general counsel would be advised to review the existing crisis management plans, or design a new one from the bottom up.

Crisis Management Planning

When your company has a computer intrusion incident, most experts conclude that it is a question of when, not if, you deal with the aftermath. The crisis management plan is the playbook companies follow to resolve computer intrusion incidents. Thus, the general counsel needs to ensure that the company creates a crisis management plan in advance of any incident. The purpose of a crisis management plan is to limit the "chaos" of an intrusion event, restore computer services, investigate the incident, and prevent future problems, in that order.

When a proper plan is in place, your company can preserve resources and maintain infrastructure stability. Moreover, a proper plan will preserve valuable data, i.e., evidence, that will be needed both to recover the systems and to conduct a proper investigation. Planning is not enough. A responsible strategy includes putting the plan into action—conducting a fire drill. The routine practice of executing the

crisis management plan will keep the company sharp and ready in the event of a catastrophic event. The focus of the fire drills should be organizing the crisis management team, identifying key participants in the process, and creating a plan of action, as described in more detail below.

- Identify a crisis management team. A crisis management plan needs to be prepared and executed by a crisis management team. The team members must have clear identifiable roles that are related to the specific crisis management goals. Specifically, a well-defined team should be broken down into at least three distinct function groups: 1) the recovery group, 2) the investigation group, and 3) the prevention group. There should be at least one person with the

The starting point for any general counsel is to obtain a basic understanding of the company's network architecture.

authority to oversee all three functions. This crisis manager will be responsible for securing resources and vested with the authority to ensure that each group has the resources and expertise to complete its task.

Ideally, these three groups should work independently from each other, as discussed in more detail below. In addition, the plan should include key internal participants from other corporate departments including: (1) public relations, (2) corporate governance, (3) in-house counsel, (4) human resources, (5) IT and engineering, (6) corporate security (physical and computer), and (7) customer services. In a well-designed plan, other key internal corporate participants will act to support the activities of management and the crisis team. In order to work effectively, the crisis management plan should identify, group by group, and periodically update, its list of external experts who may be necessary to assist in resolving the crisis.

The recovery group includes system administrators and engineers who are familiar with your system; internal customer service representatives; incident response experts; computer hardware and software vendors; archive data resource persons.

The investigation group includes computer forensics experts; physical security experts; outside counsel; law enforcement contacts.

The prevention group is made up of computer intrusion prevention experts; internal IT and security professionals.

- Ensure that knowledgeable internal IT personnel are involved at all stages. The crisis management plan should include internal IT personnel whose function is to interact or liaise with non-computer

technical participants—both internal and external. For instance, if in-house counsel is dealing with outside counsel or computer forensics experts, an internal IT professional should be involved to ensure that there is complete understanding of technical matters and data.

- Identify critical intellectual property, know-how, and infrastructure. In designing a crisis management plan, general counsel would be wise to consider and identify the key computers that have the greatest impact on the company's operations and other important corporate functions. Consider these targets as the crown jewels that should be protected at all costs. In addition, keep in mind that certain intellectual property and know-how may be just as important to the company's operations. For instance, if you represent a hedge fund that uses a complex trading program or algorithm, is that intellectual property properly protected within the network from computer intrusion?

Finally, be mindful that in any computer intrusion prosecution, the government must establish and prove how the intrusion occurred and by whom it was done. Invariably, this requires the government to show the public how the defendant improperly breached the company's security system. Companies have legitimate concerns about how much detail has to be disclosed in order to satisfy the government's burden of proof. For instance, is the government required to disclose Internet Protocol addresses of all the relevant computer systems? Is it required to disclose certain critical infrastructure information or IP assets? Prior to commencing litigation or making a criminal referral, make sure that you understand what areas are critical to your client and how you can eliminate or at least minimize exposure. At the very least, you can advise your clients of the risks inherent in civil or criminal litigation.

Because most companies cannot function without computers, it is no longer optional or advisable for general counsel to sit back and wait for issues to develop. In today's world, general counsel need to go out and become engaged in IT issues now and join ranks with the IT department's efforts to ensure a secure computer network environment. In many cases, only general counsel will be able to detect long-term litigation risks that the IT department is not trained to detect.