WHAT BUSINESSES SHOULD KNOW ABOUT CYBERTERRORISM

By Peter K. Yu

Introduction

The terrorist attacks on the World Trade Center and the Pentagon and the plane crash in rural Pennsylvania resulted in a tremendous loss of life, property and money and created psychological distress on people around the world. Within hours, downtown Manhattan was transformed from the United States' financial capital and one of the world's major tourist attractions to an evacuated war zone with collapsed buildings, burning rubble, a tower of smoke and mountains of broken glass, concrete and debris. Thousands of innocent people were killed. Tens of billions of dollars were lost. And an incalculable amount of business documents were incinerated.

While the effect of these attacks was devastating, physical destruction is but one form of terrorism. Of increasing concern is a new form of terrorist attack known as cyberterrorism, which seeks to damage and incapacitate computer networks and telecommunications infrastructures and to compromise secure data stored in information systems. These attacks range from sophisticated strategic information warfare backed by hostile state actors and terrorist groups to amateur "hacking" of computers by a small group of individuals who happen to obtain access to some "cyberattack" software available on the Internet.

Today, virtually all critical infrastructures in the United States are connected through a cooperative network of computers, information systems and telecommunications infrastructures. Damages inflicted upon a single point of entry can easily destroy the entire system and wreak havoc on adjacent networks that interact with the system. Attacks on data and information systems therefore can be just as destructive as attacks on buildings and physical infrastructures.

In fact, cyberterrorism could cause massive injuries and a substantial loss of human lives. For example, a cyberterrorist could reroute 911 emergency calls to telephone numbers for sex service, alter medical records in clinics and hospitals, and cause fire and explosion by misadjusting pressure on electrical pumps. A cyberterrorist also could throw air traffic control centers into chaos and paralyze shipping and railroad computers. By hacking into computers in the Pentagon and other similar military facilities, a cyberterrorist could even deploy troops and initiate weapons of mass destruction. In light of the potential for large-scale destruction, the government and the private sector have been particularly concerned about cyberterrorism.

In the United States, the private sector owns or manages a large number of critical infrastructures, including banking and finance, electricity, oil and gas production, telecommunications, transportation and water supply. Because of the importance of these infrastructures to the country's economy and their close relationship to national security, the private sector increasingly has been targeted for terrorist attacks. Unfortunately, many business managers are unaware of the danger of cyberterrorism and the vulnerability of their computer systems. They therefore fail to take the necessary precautions that may help prevent, or mitigate damages caused by, cyberterrorist attacks.

Moreover, the costs of hardware and software have decreased significantly, and information about how to attack computer networks are easily and readily available on the Internet. Even worse, powerful search engines provide a lot of information about web sites that may be targeted for cyberterrorism and allow terrorists to compile the data needed for potential attacks. Thus, today's cyberterrorists and hackers are no longer confined to students with high intelligence and very impressive computer skills. Rather, they include people from all walks of life, including computer scientists, computer security specialists, disgruntled employees, foreign spies and military personnel, criminals and fraud perpetrators, political activists, and even young teenagers with very limited computer expertise.

Insurance Protection

The most common technique for protection against threats—whether from cyberterrorists or other, more traditional sources—is through insurance. Cyberterrorism can cause damages in two ways. First, it can destroy information systems and telecommunications infrastructures by physical attacks, such as bombing, arson and destruction of property. Second, it can damage computer networks through unauthorized access to the system, which is generally known as "hacking" (or to be more precise—"cracking"). To protect themselves, businesses should ensure that there is sufficient insurance to cover both types of attacks. (Some insurance carriers may require special "hacker insurance," which protects against damages caused by unauthorized access to computer networks.)

To plan for contingencies that might arise from cyberterrorism, businesses should assess their vulnerability to cyberterrorist attacks. For example, big companies are in general more vulnerable to cyberattacks than small companies, partly because of their national (or international) reputation, the indispensable nature of their services and the substantial relationship some of them have to national security. Sophisticated computer security systems and the ability to attract media attention also present attractive challenges for cyberterrorists. Small companies also may be affected because their computer facilities are located in close proximity to big companies or because they subscribe to the same information network or service or content providers as the big companies.

To ensure adequate protection, businesses must understand the nature and scope of their insurance policies and the potential coverage. They must pay attention to the various exclusions that apply to their coverage. Courts tend to resolve ambiguities in an insurance policy in favor of the insured. For example, a majority of courts require insurance carriers to prove the existence and operation of a specific exclusion. However, a small minority of courts has shifted the burden of proof to the insured once the insurance carrier establishes satisfactorily that a specifically asserted exclusion applies.

Among the various exclusions, those relating to war and terrorism warrant special attention.

In the past, the U.S. government generally defined terrorist attacks as criminal acts, which were to be dealt with by law-enforcement agencies. This definition made it difficult for insurance carriers to deny protection by applying the war exclusion. However, with respect to the recent terrorist attacks, the Bush administration has described them as "acts of war." In light of this

changing definition, insurance carriers may have a stronger argument for invoking the war exclusion.

Nevertheless, given the present turn of events, the major insurance carriers would unlikely assert this exclusion lest they damage their business reputation and long-term profits. The Federal Emergency Management Agency (FEMA) and other government agencies also may offer to cover some of the losses should the insurance carriers be not able to do so.

Terrorist activities are generally rare and their damages unpredictable. Thus, insurance carriers rarely factor terrorism into insurance premiums. However, if terrorist attacks occur more frequently, insurance carriers may change their policies by including a terrorism exclusion, which would exempt the carriers from liability for any damages caused by terrorism. They also may set a limit to the insurance coverage concerning damages caused by terrorism or increase the premiums by building terrorism into the pricing mechanism. After all, the recent attacks have demonstrated that terrorism can inflict massive calamity and war-like damages.

Precautionary Measures

Insurance is not the only way businesses can protect themselves against cyberterrorism. Indeed, insurance may not be able to cover all the potential damages and losses. To fill these gaps, businesses should take the following precautions.

Large companies should secure alternative computer facilities that would allow them to continue operation in the event of a terrorist attack. Immediately after the attack on the World Trade Center, many companies relocated (temporarily) to offices in nearby cities in the tri-state area of New York, New Jersey and Connecticut.

However, not all companies can afford to maintain alternative facilities. Thus, businesses should consider negotiating a mutual arrangement with an industry partner (or even a business competitor) to deal with emergency situations caused by cyberterrorism. This arrangement, which serves the same purpose as maintaining an alternative facility, may cause a company to incur financial costs. However, these costs can be easily covered by insurance and, in most events, would be lower than the financial loss resulting from continuous business disruption.

To protect against the irretrievable loss of important documents, business information and financial data, companies should make backup copies of their records frequently and store them in an offsite location or with a secure third party. Sound information system management practices recommend the creation of backups at least once a day. Should a terrorist attack occur, the company could resume its business within a short period of time by using these backup copies.

Furthermore, businesses should design emergency plans that include alternative suppliers, service providers and content providers that are located outside the area in which the business resides or that use a different information network or telecommunications infrastructure. By doing so, the recovery of the business would not be dependent upon the successful recovery of its suppliers and service and content providers.

Finally, whenever and wherever possible, businesses should strengthen the security of their computer networks. Examples of precautionary measures include:

- install firewalls to protect computer networks against unauthorized access;
- limit access to computing and information resources to authorized personnel only;
- encourage, or even require, users to change passwords frequently;
- conduct regular background checks of employees in sensitive positions;
- install audit features that monitor log-on and log-off activities;
- provide warnings that unauthorized users may be subject to monitoring and prosecution;
- develop a trap and tracing mechanism with local telephone companies and implement systems that identify outside callers;
- report significant security breaches to relevant government agencies;
- implement policies and guidelines regarding the use of computing and information resources by employees;
- identify and implement controls over external access to internal networks (through dial-in modems and extranets);
- install antivirus software and require employees to scan all software and electronic files received from outside sources;
- encourage employees to use encryption technologies if appropriate;
- implement security upgrades when they become available;
- increase awareness among users of cyberterrorism and the importance of computer security; and
- communicate with other members of the industry and computer security professionals regarding best practices to protect computer networks and possible cyberterrorist attacks.

Government Actions

In addition to the private sector, terrorism has the potential to cause significant damages to the general public. To protect its citizens, the government may put up efforts that help prevent or eradicate terrorism.

Most of the time, these efforts call for changes in the business environment. Sometimes, these changes are controversial and may require businesses to change their existing policies. For example, to allow for stronger surveillance of suspected terrorists, the government may ask companies to release sensitive personal information and business data to government investigators, thus calling into question the company's fiduciary obligations. The government also may prohibit the use of certain encryption technologies and even may mandate specific standards and information practices that would accelerate the information-gathering and investigation processes. To avoid any further complications and later modifications, companies should work closely with government agencies to develop standards and practices that protect the general public against terrorist attacks while causing minimal damages and inconvenience to the businesses community.

Moreover, despite the government's well-intentioned efforts to protect its citizens, these efforts sometimes may infringe upon consumers' privacy and civil liberties, thus making consumers more reluctant to continue their existing lifestyle, conduct business through the Internet or

provide companies with accurate and reliable personal information. To alleviate this problem, businesses should actively review and assess the government's proposals and discuss their concerns and the practicability of the proposed standards and practices with the government.

***

Terrorist attacks are destructive, despicable and diabolical. Yet, they are a reality, especially for businesses in the United States and other Western democracies, which are repeatedly and increasingly targeted for terrorist attacks. Although it may be difficult to eradicate terrorism, businesses can take proactive measures to prevent cyberterrorist attacks and mitigate damages resulting from these attacks.

In the New Economy, where virtual corporations and cash-free electronic transactions are vital to business success, cyberterrorism can cause tremendous damages. Thus, the government and the private sector should work closely with one another to develop a defense system that protects the computer networks, information systems and telecommunications infrastructures against cyberterrorist attacks.

Peter K. Yu is a member of the GigaLaw.com Editorial Board and the executive director of the Intellectual Property Law Program and deputy director of the Howard M. Squadron Program in Law, Media & Society at Benjamin N. Cardozo School of Law in New York City. He is a research associate of the Programme in Comparative Media Law & Policy at the University of Oxford and has written on a variety of legal topics. He is licensed to practice law in the state of New York. E-mail: peter_yu@msn.com.