LegalTimes WEEK OF January 19, 2004 • VOL. XXVII, NO. 3

Securing Our Cyberspace

The private sector needs to protect itself—and the nation—from computer threats.

BY JAMES S. GILMORE III,
JOSEPH T. CASEY JR.,
AND STEPHEN M. ARNER

In the wake of the Sept. 11 attacks, the U.S. government, state and local governments, and private industry have turned their attention to making their segments of cyberspace—the universe of computers connected through the Internet and other networks—as secure as possible. For businesses, the question is not *whether* those in the private sector face potential liability for failing adequately to secure their respective segments of cyberspace, but rather *how* and *to what extent* such liability will be imposed.

WHAT'S AT STAKE?

Without a great deal of consideration for security, businesses in this country have fairly rapidly shifted the control of many essential processes in manufacturing, utilities, banking, transportation, and communications to networked computers. Increasingly—for the convenience of customers, to reduce costs, and other reasons—more and more processes have been networked, despite the risks inherent in allowing remote digital access.

Our networks are likely targets for a wide range of attackers, including hackers and virus writers, terrorists, economic competitors, foreign nations, criminal groups, activists, and disgruntled employees. The economic losses alone can be staggering. To take just one example, the infamous Code Red computer worm (and variants of it) infected nearly a million computers, causing an estimated $2.4 billion in damage.

Other recent attacks have resulted in less easily quantified, but nonetheless potentially severe, consequences. For example, a hacker broke into the University of Washington Medical Center's networks and downloaded private admissions records for more than 4,000 patients.

A few recent attacks have also had concrete effects on physical (as opposed to virtual) infrastructure. For example, a computerized waste management system in Queensland, Australia, was hacked in 2002, causing millions of liters of raw sewage to spill out into local parks, rivers, and the grounds of a hotel. And several years ago in Massachusetts, a local telecommunications system was hacked, disabling local phone service, which in turn deactivated automated systems controlling lighting on runways at the local airport, forcing the airport to close.

As our dependence upon cyberspace continues to expand, the sophistication, severity, and frequency of attacks on our cyberspace is also increasing. According to a report issued last year by the U.S. General Accounting Office, the number of reported computer security breaches rose to 82,094 in 2002, and it is believed that as many as 80 percent of security incidents are not reported. The likelihood of cyberattacks (or severe outages) resulting in possible widespread destruction or deaths grows accordingly.

The overall impact of a severe attack is unknown, but what is known is that attacks will continue to be directed against this nation's cyberspace. It is feared that al Qaeda and other terrorist organizations will turn to cyberattacks in their ongoing attempts to damage this country's economy and to cause destruction. In the week following the attacks of Sept. 11, 2001, the Federal Bureau of Investigation warned of the possibility of a "digital continuation" of the attacks. Later that year, investigators discovered a house in Pakistan devoted to cyberwarfare training. Information on U.S. computerized water systems was found on computers in al Qaeda camps in Afghanistan. It is feared that terrorists may seek to augment physical attacks with cyberattacks—by stranding subway cars and disabling emergency response systems with a cyberattack prior to detonating an explosive, for example.

In short, failures to adopt and implement cybersecurity plans could have grave consequences. As a result, whether an attack results in economic damages to a few parties or widespread physical destruction, the exposure for businesses that fail to take reasonable security measures is tremendous.

POTENTIAL SOURCES OF LIABILITY

State negligence law provides one framework for imposing liability upon entities that fail to take reasonable cybersecurity measures. Companies that fail to provide reasonable security in the face of cyberthreats—by allowing their networks to be used to launch attacks against others or their data to be altered or destroyed, for example, as well as companies that negligently design or maintain software or hardware—should expect to face

liability under state law negligence actions. Such suits are inevitable. In determining the standard of care to apply in such actions, courts are likely to turn to several available sources in the absence of laws explicitly addressing liability in cyberspace.

First, courts are likely to look to regulations that govern specific industries, such as the health care and financial services industries, which generally do not specify particular security measures that must be adopted, but rather describe a security process by which businesses should assess risks, develop and implement security plans, continually monitor their networks, and reassess and as necessary revise their security plans. Laws setting forth such standards include the Health Insurance Portability and Accountability Act of 1996 and the Gramm-Leach-Bliley Act of 1999. Such regulations will likely provide some guidance as to what is reasonable and feasible, even in the context of industries that are not directly subject to the regulatory provisions.

Similarly, actions of the federal government concerning the security of its own computer networks may provide guidance as to what will be reasonably required of private industry. (Though should the government continue to fail to reasonably secure its portion of cyberspace, private industry should not assume that such failure will insulate business from liability.)

The Bush administration's approach to cybersecurity, as set forth in its 2003 National Strategy to Secure Cyberspace, has been criticized in some quarters for failing to impose any specific mandatory requirements for the provision of cybersecurity upon private industry, echoing the "hands-off" approach espoused by the prior administration. Rather than mandating specific security measures (such as the provision of firewalls and anti-virus software to customers by Internet service providers), the National Strategy indicates that the federal government will lead by example, securing its own segments of cyberspace, while encouraging the private sector to "secure the part that they own or for which they are responsible."

Although the National Strategy does not require the use of specific security measures, it nonetheless may be a source of information as to what may be required. The National Strategy describes the process by which the government will seek to protect its own segments of cyberspace and describes certain specific measures that will be considered (such as multilayered identification and authentication). The National Strategy also indicates that the federal government will use its procurement power indirectly to impose security standards by requiring parties that contract with the government to adopt reasonable cybersecurity measures and to develop "best practices" for certain systems.

The National Strategy, therefore—especially when viewed in conjunction with President George W. Bush's December 2003 directive calling for the development and implementation of uniform policies, approaches, guidelines, standards, and methodologies for securing the federal government's networks—is at a minimum likely to influence development of an appropriate standard of care for cybersecurity efforts by private industry.

Other possible mechanisms by which businesses may be held liable for cybersecurity failures include actions for breach of contract (reasonable cybersecurity measures are increasingly required in contracts), enforcement of consumer protection statutes (requiring businesses to abide by voluntary commitments made, for example, in public privacy policies), enforcement of industry-specific standards (either voluntary standards adopted by industry groups or industry-specific regulations), and securities laws (requiring disclosure of material risks).

Finally, although the National Strategy expressly disavows any intention to use direct regulation as the means of securing cyberspace, should industry fail adequately to move forward on cybersecurity issues, the National Strategy acknowledges the possibility that legislation and regulation may prove necessary.

How Much Security?

Because much of this nation's cyberspace is owned and controlled by the private sector, the private sector is best equipped and structured to take reasonable steps to respond to the evolving cyberthreat. But what are the "reasonable steps" sufficient to satisfy the developing standard of care needed to avoid liability?

It is impossible to make computer networks 100 percent secure. Absolute security, therefore, cannot and will not be required, and the mere fact of a successful cyberattack will not be sufficient to serve as the basis for the imposition of liability. Rather, what will be required of businesses is the development and adoption of a process to protect their computer networks, the reasonableness of which will be judged by balancing the likelihood that cybersecurity breaches will cause harm, the expected extent of such harm, and the burdens that would be imposed in attempts to prevent such security breaches. Different entities will thus be held to different standards, because of the differences in risks and burdens.

The details vary case by case, but generally, businesses should, at a minimum, undertake the following steps to secure their portion of cyberspace:

- Inventory and assess assets.
- Conduct a risk assessment.
- Develop a thorough written cybersecurity plan.
- Designate specific individuals responsible for cybersecurity.
- Institute training programs to ensure knowledge of and compliance with the security plan.
- Continually monitor, probe, and test computers and networks.
- Oversee third parties' compliance with the cybersecurity plan.
- Implement reasonable physical, administrative, and technical security measures.
- Provide for disaster recovery.

By addressing cybersecurity now, businesses can minimize their potential liability exposure. Counsel can assist with the development and implementation of corporate cybersecurity plans by tracking judicial, legislative, and regulatory developments and assisting in the evaluation or development of a written security plan. Similarly, counsel can evaluate and draft contractual instruments governing relationships with third parties in order to ensure that cybersecurity is adequately addressed, can assist businesses in insuring against cyberrisks, and can assist when cybersecurity failures inevitably occur.

James S. Gilmore III, the former governor of the Commonwealth of Virginia, is a partner in the D.C. office of Kelley Drye & Warren, where he chairs the homeland security practice group. Since 1999, he has been chairman of the Congressional Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. Joseph T. Casey Jr. is a partner in the Tysons Corner office of Kelley Drye, where his practice focuses on government contracts, commercial litigation, and defective-software disputes. Stephen M. Arner is a litigation associate in the Tysons Corner office of Kelley Drye.