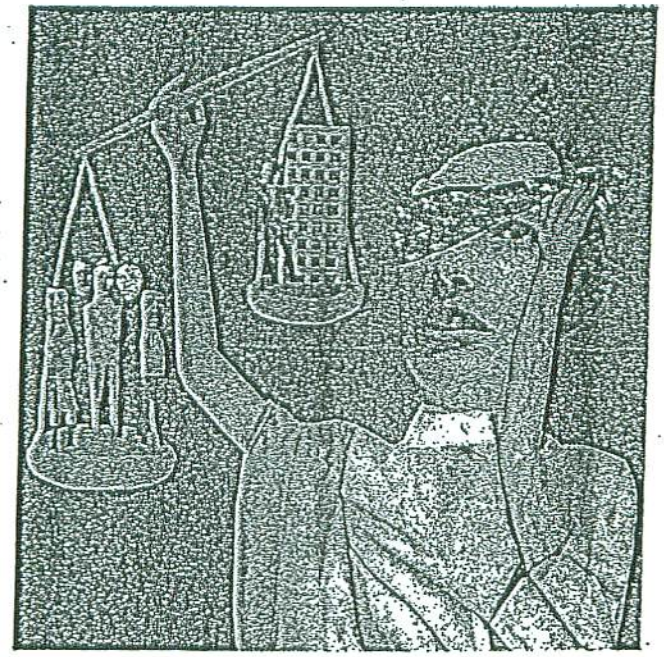
A Foreseeable Future

For liability purposes, the courts have declared terrorism to be a predictable security threat. Our new legal columnist advises CSOs to adapt if they want to survive.
By William Cook

THE CONVENTIONAL WISDOM in the weeks and months after Sept. 11th was that no one could have predicted the events of that day. The use of airplanes as weapons was roundly declared an asymmetrical threat. However, two recent court cases have altered the legal definition of a "foreseeable event."

In the class-action litigation brought by families of Sept. 11th victims against the airlines, airport security companies, airplane manufacturers and the owners and operators of the World Trade Center, the court examined two main elements: 1. Whether the various defendants owed a duty of care to the people in the World Trade Center and on the planes that crashed; and 2. Whether the terrorist act was foreseeable. In finding that the case should go to a jury, the court stated that we impose a duty on a company when the relationship between the company and user requires the company to protect the user from the conduct of others. The court noted that we already depend on others to protect the quality of our water and the air we breathe. This duty of care extends to private companies.



But the court also made a revolutionary declaration with respect to foreseeability. The court stated that, typically, a criminal act (such as terrorism or hacking) severs the liability of the defendant, but that doctrine has no application when the terrorism or hacking is reasonably foreseeable. The court went on to note that the danger of a plane crashing if unauthorized individuals invaded the cockpit was a risk that the defendant plane manufacturer should reasonably have foreseen—indicating that terrorist acts are indeed foreseeable.

The second case involved Verizon and the Maine Public Utilities Commission. The case dealt with whether Verizon could get a waiver for certain performance failure penalties that it was required to pay. Verizon argued that it should not have to pay, since its website went down due to the Slammer worm. The commission found that viruses and worms are foreseeable events, as evidenced by the regular security bulletins issued by software companies. The commission found that Verizon had not taken the reasonable steps available to it; steps that competitors AT&T and WorldCom did take (installing patches to ward against Slammer). Ultimately, the commission found that Verizon should be held accountable for its failure, indicating that virus attacks are also completely foreseeable events.

So now that threats to technology and other systems are no longer considered unforeseeable, what is a conscientious CSO to do?

Three suggestions. First, companies must have "court provable" security. They must be able to prove they use best practices with respect to policies for information management, security, implementation of those policies and disaster recovery plans. When a company gets sued as a result of a security breach, it goes a long way in court if the company can show that it established and followed nationally recognized security policies and procedures.

Second, buy cyberinsurance from a trusted broker with a national or international underwriter.

Third, consider buying antiterrorist technology. Under the Support Anti-terrorism by Fostering Effective Technologies (Safety) Act, sellers of qualified antiterrorism technology (QATT) are provided with risk and litigation protections. In a nutshell, it encourages the development of antiterrorism technology by providing liability limits for terrorism claims.

Relying on the disaster-recovery policy buried on the CEO's desk won't cut it. Security breaches have never been more highly scrutinized by the courts and regulators, and they are redefining what companies should have seen coming—be it a stolen aircraft or a computer virus. Implementing the right policies, procedures and technology now can limit your company's liability in the future. ■

Send any feedback or topic suggestions to Senior Editor Daintry Duffy at *dduffy@cxo.com*.

CSO Welcomes a New Flashpoint Columnist

William Cook is an attorney specializing in intellectual property litigation, business continuity and security with Wildman Harrold Allen & Dixon based in Chicago. Cook is also president of Infragard-Chicago and a founding member of the U.S. Secret Service Chicago Electronic Crimes Task Force.

ILLUSTRATION BY KATHERINE STREETER