



Career Corner

Information Security and the Law: Part Two of a Two-Part Series

By Joyce Brocaglia

Note that this is just a general overview of legal and security issues and is NOT legal advice. Anyone with questions in this area should contact their own attorney.

This conversation with Randy Sabett is the second installment of a two-part series that addresses legal topics that are on the minds of information security executives everywhere. Randy V. Sabett, J.D., CISSP, is an associate in the Information Security and Cybercrime practice group of Cooley Godward LLP and a member of the firm's Technology Transactions Group. He is a Co-Vice Chair of the Information Security Committee of the Section of Science and Technology of the American Bar Association and teaches information policy as an adjunct professor at George Washington University.

JB: What effects will the Department of Homeland Security have on private sector companies?

RS: The Department of Homeland Security (DHS) provides an opportunity for private sector information security companies to supply innovative and cost-effective solutions to specific governmental problems. These companies, however, will be subject to some additional requirements and compliance. For example, under the Federal Information Security Management Act (FISMA), the information systems of all contractors will need to meet specific security requirements. In addition, DHS may influence the legal process and impose requirements that are above and beyond the current slate of laws that impose information security requirements (for example, SB 1386, HIPAA, GLBA, SOX, etc.) The DHS recently made two significant announcements in the cyber security area. First, Amit Yoran has been appointed as the new leader of the National Cybersecurity Division of DHS. Mr. Yoran formerly served as the Vice President of Managed Security Services at Symantec. Mr. Yoran, a seasoned security professional, will provide DHS with a unique perspective because of his commercial background. Second, a DHS incident response center has been established. Known as the U.S. Computer Emergency Response Team (US-CERT), it represents a very positive step toward public and private sector coordination.

JB: What about the critical infrastructure? Do we really need to be concerned?

RS: Numerous components of the country's critical infrastructure could be subject to attack by any of several different entities. These include script kiddies, individual hackers, elements of organized crime, nation states, and terrorists. Although no publicly known organized attacks have occurred on the critical infrastructure, there have been enough individual attacks to demonstrate that significant vulnerabilities exist. As just one example, a case currently being tried in the U.K. involves an English hacker that was in love with an American woman. A person in a chat room wrote disparaging remarks about the U.S. that prompted an argument with the hacker. The hacker then launched a denial of service attack that targeted the chat room person, but which wound up also bringing down the Port of Houston in September of 2001. The attack crippled the port's communications system, causing several ships to be put into potential danger because of the

unavailability of weather and navigation information. Although there were no major problems, this is believed to be the first known cyber attack on a component of the country's critical infrastructure.

JB: With all this talk about wireless security, do I really have anything to worry about from a liability standpoint if my company allows its use?

RS: Companies must balance the convenience and speed with which a wireless network can be brought up against both the nature of the information on the wireless network and the ability to secure the wireless network. Allowing a wireless network to be deployed within a company, even if it is without the company's knowledge, could expose the company to liability. If, for example, high-value information resides on the network and an attack occurs over a known or unknown wireless network that an employee happened to set up, the company could wind up liable for unauthorized disclosure of the information. A company that definitely wants to deploy wireless capability, however, can consider various techniques for protecting the information. Although WEP does contain flaws, the company could implement it as a minimum level of defense. The company might also contemplate encryption of all sensitive information on the network servers (or at least the information deemed to be of high enough value). The company might further consider physical separation of data, so that the high-value data resides on a network that cannot be reached from the external network (though the latter two examples could have an adverse impact on performance). Finally, the company might deploy any of several new security solutions that provide protection that is specific to a wireless environment. These include, for example, wireless MSSPs that can detect rogue access points or rogue wireless users and software that can lock down the authorized wireless clients by closing all unused ports and automatically setting up the configuration of the wireless client for known and unknown access points.


JB: What are some other hot legal issues in the information security space?

RS: One of the hottest issues right now is the potential class action lawsuit that was filed against Microsoft in October of 2003. The suit alleges that the personal information of at least one plaintiff (and perhaps as many as several million) was compromised as a result of alleged weaknesses in Microsoft products. There are several claims asserted against Microsoft, including one that is based on the California privacy law (SB 1386). Many commentators have predicted that the actual legal contours of SB 1386 cannot be discerned without companies resorting to litigation. This case may provide the first insights into how the courts will apply and construe the law.

A second very hot infosec issue involves digital evidence and its changing nature. Unlike tangible evidence, for which only one true original exists and is difficult to counterfeit or reproduce, evidence in digital form can, without proper controls, be easily copied, altered or misused. The Information Security Committee within the American Bar Association is currently working on a comprehensive and seminal work known as the Digital Evidence Project. It

will examine all of the issues related to digital evidence and lay out the contours of where and how the law could develop.

A third issue involves allocation of liability and the use of insurance for cyber risks. Several insurance companies offer standard technical errors and omissions policies. Others may tailor specific packages and policies based on specific risks. Still others who are very well-versed in the security area offer specific cyber risk policies that may cover a number of the different types of compromises that could occur. As with all such policies, though, you should review them carefully to ensure that they adequately address the possible cyber risks that your business may face.

A final area with significant activity is the field of identification technology. Recent government reports and testimony have revealed the ease with which falsified identification papers can be obtained. The liability associated with such activity could be significant. To demonstrate the severity of the problem, consider the following: an October 1, 2003 report from the Government Accounting Office states that “[t]ests we have performed over the past 3 years demonstrate that counterfeit identification documents can be used to enter the United States, purchase firearms, gain access to government buildings and other facilities, obtain genuine identification for both fictitious and stolen identities, and obtain social security numbers for fictitious identities.” Though the news is somewhat thought-provoking, it didn’t really reveal anything new. We have known for years that false IDs can be procured easily. Solutions are needed that provide adequate authentication. Numerous technologies, including many involving biometrics, can provide this type of authentication. 

*Joyce Brocaglia is the CEO of Alta Associates, the Human Capital Risk Managers specializing in information security recruiting.
www.altaassociates.com*