



Career Corner

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

By Joyce Brocaglia

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

With the increase of regulatory demands placed on the information security industry, numerous executives are asking *what potential legal effects could this have on my company and me personally?* I turned to Randy Sabett, J.D., CISSP, is an attorney 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. Here's what he had to say.

JB: What kind of liability could my company face as a result of a security breach?


RS: *Any number of legal theories could be applied in a situation involving a security breach. Unless a contractual relationship exists between the entities involved, one of the most likely theories would be the tort law theory of negligence. Under such a theory, a plaintiff (i.e., wronged party—the victim of the information security breach) would claim that (a) the defendant (i.e., the alleged wrongdoer) had a duty to protect the plaintiff, (b) the duty was breached by the defendant, (c) the breach led to harm to the plaintiff, and (d) the plaintiff suffered damages as a result. If the plaintiff were to prove all of these elements, he or she would prevail on a negligence claim. There are, however, certain problems that exist. For example, many courts do not recognize purely monetary damages as actionable under a negligence theory.*

On the other hand, if a contractual relationship exists between the parties, any number of contract provisions could be breached as a result of a violation of a company's information security. For example, unauthorized access to data could lead to an allegation that a confidentiality provision was violated. Similarly, a breach that slows down the system (for example, one of the recent worms or viruses) could lead to a breach of a service level agreement.

Finally, there could be civil liability under statutory law (i.e., persons might be able to bring a cause of action against a company because the law specifically states that they could do so). For example, the Computer Fraud and Abuse Act (18 U.S.C. 1030—see <http://www4.law.cornell.edu/uscode/18/1030.html>) allows a person to bring a civil action against an alleged wrongdoer if the provisions of the law are violated.

JB: Can a CSO be held personally liable?

RS: *As a practical matter, whether and when a CSO has personal liability for a breach of security will largely be determined by whether the person was acting within the scope of their employment. If a breach of security occurred that led to a third party being harmed, as long as the acts were not intentional or criminal and were within the scope of the*

CSO's duties to the company, the CSO would likely be protected by the insurance coverage of the company (for example, a D&O or E&O policy). Even if insurance coverage isn't available, where acts are within the scope of employment, the company, not the individual, is usually the appropriate defendant and individual defendants are often dismissed from the lawsuit before trial. Where third-party claims are brought against an individual based on actions which took place within the scope of employment, most employers provide a defense for their employees. From a proactive perspective, the CSO could ask for an indemnification agreement from the employer which requires the employer to take responsibility for third-party claims. If the acts of the CSO were criminal, however, that individual could be subject to individual liability under specific laws related to security breaches (most notably the penalty provisions of HIPAA for unauthorized use of personally identifiable health information). 

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