

Corporate Preparation & Response to Hacker Attacks

Every day brings more *Wall Street Journal* coverage of new computer break-ins or an update on earlier break-ins that are worse than previously thought. This rash of heavily publicized hacker attacks on corporate systems has corporate managers questioning how safe their systems are, what they can do to prepare in advance for an attack, how they should respond, and what their liability exposure might be in the event of an attack. Additional issues include: what can be done to protect consumers, customers, and trade secrets; reduce losses; minimize potential damages; protect shareholder value; and otherwise control the problem as much as possible. Some due diligence steps that should be taken include the following:

1. Set up an intracorporate Emergency Response Team now, in advance of any attack. Do not limit its members to IT staff. Effective incident response requires a broad range of corporate talent. Include the corporate risk manager, corporate privacy officer, compliance director, CFO, HR department, the company's physical security director, an in-house spokesperson and in-house counsel. Document each person's duties. The CEO and the corporate board should be advised and sign off on the make up of the Response Team and their authority.
2. The Response Team should meet monthly to go over contingency plans and review the current intrusion trends. These meetings should also contain a report from the IT staff about what type of probing the network is receiving from the Internet. Unusual IP addresses that are repeatedly probing the system should be noted. In the event of an intrusion, the Team can quickly form an organized response that minimizes losses and confusion and makes decision about contacting law enforcement agencies, determines whether outside forensic assistance is necessary and determines immediately if customers need to be alerted to any data compromises.
3. Only one person speaks to the press. The company spokesperson clears all comments through the Response Team and upper management.
4. The Response Team should reach out and identify local law enforcement agents such as the FBI, the U.S. Secret Service or local police cyber teams before any break-in. Join private sector reach out programs sponsored nationally by these agencies such as the FBI InfraGard program, and U.S. Secret Service Computer Crime Task Force. A Response Team member should attend the quarterly meetings of these groups to get updated information about current cyber attacks and to gather business cards from agents that specialize in countering cyber attacks. Once you return to the company, circulate the meeting results and the agent contact information to other members of the Team.
5. Consider the rapidly expanding corporate liability for protecting personal information. Twelve states require corporations to provide security for personal information. Three states impose a specific duty to protect credit card information. Additionally, six states require the encryption of personal information held by companies. As a result, inside the company, identify, isolate and/or encrypt the critical assets of your company. This includes stored trade secrets, emails regarding advanced project research, patent research, customer lists, employee healthcare information, stored credit card information and any personal information you save on your customers and employees.
6. Insure that outside corporate vendors have security that meets or exceeds your security standards.
7. At one level, computer security is a check off the box exercise. Determine a recognized computer security program that applies to your industry and corporate activities. Apart from the Payment Card Industry Data Security Standards used to protect credit card information, most security standards such as HIPAA and NEST will provide you with a flexible standard that can be used across the company and

achieve “reasonable security under the circumstances.” After the boxes are checked, steps need to be taken to insure that internal security standards are actually being applied.

8. Discuss with outside legal counsel, as part of their cybersecurity audit, the advisability of having them hire an outside forensic company to “tiger team” your system for potential holes. They should conduct penetration tests, scan your systems for vulnerabilities and map out your network structure. Their report to legal counsel should be evaluated and used as actions items by the corporate Response Team.
9. Obtain, or at least evaluate obtaining, intrusion insurance. The costs are coming down for insurance products offered by some of the largest and smallest carriers.
10. Have the Response Team prepare potential media responses that account for various scenarios: lost trade secrets, lost consumer information, denial of service attacks, etc. Spontaneous comments are no good and “no comment” will often lead to reporters contacting employees for informal comments. It’s better to have a corporate response that is thought out and appropriate if questions are asked.
11. Recognize that in almost all states, consumers whose information has been lost or compromised will have to be quickly notified about the breach. As soon as an event happens, the Response Team needs to start tracking the names of consumers who have been put at risk.
12. If your company webpage has advertising, make sure you know who is placing the advertising on a continuing basis. “Malvertising” is a growing threat to consumers who go to your webpage and trust you to secure your site.

Perfect information protection is not possible and the evolving nature of hostile technology is reflected by the daily news. But, keep in mind, corporate protection from liability is established by a showing of due diligence both before and after a computer intrusion.

McGuireWoods Global Data Security Team

Counseling regarding data protection, including global data breach and privacy issues is one of the services of McGuireWoods’ interdisciplinary Technology & Outsourcing practice. For assistance on UK and EU data protection matters, contact Phillip Rees in London at +44 (0)207 632 1600. For assistance in the United States on export control and data breach issues, contact Bill Cook in Chicago at 312.750.2750 or Janet Peyton in Richmond at 804.775.1166. For assistance with other business matters driven by technology, contact Steve Gold, chair of the Technology & Outsourcing Practice at 312.321.7664.

If you would like to receive our legal news updates by e-mail, please sign up online at www.mcguirewoods.com.



McGuireWoods news is intended to provide information of general interest to the public and is not intended to offer legal advice about specific situations or problems. McGuireWoods does not intend to create an attorney-client relationship by offering this information, and anyone’s review of the information shall not be deemed to create such a relationship. You should consult a lawyer if you have a legal matter requiring attention.

Copyright © 2011 by McGuireWoods LLP. All rights reserved.