CARRINGTON COLEMAN

CAPITAL

Editor: Kate Glaze

2015 Issue Three

Cybersecurity & Corporate Governance: How to Move Beyond Fear & Uncertainty to Pragmatic Solutions

By Sara Romine, CIPP/US
214.855.3103 | sromine@ccsb.com

You've read the headlines, seen the statistics, and discussed the issue with the board of directors. You get it: cyber-attacks are increasingly frequent, sophisticated, and devastating to a business's bottom line. There is no doubt that cybersecurity needs to be an important priority to the business and that real attention needs to be paid to the issue. But what does that mean? Where do you start after you've been inundated with terrifying anecdotes and the never-ending "parade of horribles" that can result from a data breach?

Unfortunately, a lot of the fear-mongering associated with cybersecurity can generate paralysis in organizations. The problem seems insurmountable and too costly to begin to address. But, in reality, there are easy, pragmatic steps an organization can take—and should take—to begin addressing its security vulnerabilities. The following are some basic measures to mitigate risk:

- **Determine the Location of Sensitive Data**. A good start is determining where your company stores sensitive, confidential, or regulated data (e.g., personal-identifying information or protected health information). Conducting a formal audit to determine the location of this data can be helpful and revealing. Legal, IT, and corporate executives might all be surprised to learn that accounting, for example, is storing bank or credit card information on an unsecure, but "convenient" drive. When reviewing the results of the audit, ask whether there is a business need to collect the information. Don't collect or retain sensitive data you don't need.

- **Assess Network Security**. At the most basic level, a company needs to ensure that its servers and network devices are securely configured and regularly scanned for vulnerabilities. The company should also ensure that it is utilizing up-to-date antivirus software, and the company's intranet is protected by a properly configured firewall. Finally, the company should determine whether its sensitive information is adequately protected when it is stored and transmitted, using strong encryption tools where applicable.

- **Monitor Network Activity**. There's a lot that can happen when no one is watching. It is critical that a company monitor its network for suspicious activities, including by using an intrusion-detection system and monitoring network logs. Knowing how network activity is logged, where those logs are stored, and how long they are available is essential to prevent and respond to a breach.

- **Restrict Access to Sensitive Data**. One of the most basic aspects of information security is implementing "security access controls"—*i.e.*, methods designed to ensure that only authorized employees are able to access sensitive data. Employees should only have access to sensitive data if there is a business reason for that access, and only a select few should have unfettered access. Restricting access helps a company monitor the flow of data, limit opportunities for piracy, and demonstrate that efforts have been undertaken to maintain the security of the sensitive data.

- **Require Secure User-Authentication Tools**. Allowing an employee to use the company name as his or her password is not much different than permitting access without a password at all. Likewise, allowing an employee with administrative access to utilize the same password for all applications, regardless of the sensitivity of information contained in each application, poses significant security threats. Instead, require employees to use complex and unique passwords

(at least eight characters, including upper and lower-case characters and numeric and special characters) and require a change in passwords at least every three months. For employees regularly accessing sensitive information, use two-factor authentication before granting access. To guard against brute-force hacking attempts, disable or suspend user credentials after a certain number of unsuccessful login attempts.

• **Vendor Security Management**. Most companies utilize third-party vendors to handle some portion of their sensitive data. If the Target data breach taught us anything, it's that third-party vendors can generate massive security vulnerabilities. When hiring a third-party vendor, be clear about your security expectations and ensure that your contract reflects those expectations (and establishes clear liability for any data breach resulting from a security breach). Develop security standards for inclusion in vendor contracts and perform audits of those security standards. Do your due diligence before hiring a vendor, especially if that vendor will be entrusted with your sensitive data or access to your network.

• **Develop an Incident Response Plan**. Let's face it, even the most dedicated and sophisticated organizations have security vulnerabilities. Every company should have an incident response plan that, in the event of a breach, clearly defines the relevant stakeholders (including the immediate involvement of the appropriate business executives, legal counsel, and relevant IT or forensics support), the role of each representative, and who is the quarterback of the response team, as well as the appropriate course of action.

• **Develop Data Destruction Policies & Procedures**. If you're going to collect sensitive data, make sure you have a plan in place to destroy the data after you no longer need it. The easiest way to limit cybersecurity risks is to ensure that sensitive data is securely disposed of once the business no longer needs it. If the sensitive data is "out of sight, out of mind," you probably don't need it and you probably aren't protecting it. Ensure that you have a procedure for identifying when sensitive information is no longer needed and a policy for securely disposing of it.

• **Train Employees and Executives!** For the policies and procedures to work, the employees and executives have to know how to apply them and be invested in following them. Security policies and procedures are simply not effective if no one knows they exist or how to implement them. Effective employee training programs will utilize realistic examples and common situations to demonstrate best practices. Likewise, employees will not follow policies and procedures unless the company consistently enforces them. Conduct formal training and reinforce the policies and procedures at every turn. ■