Practice Tips for Mitigating Data-Breach Risk and Liability

By Michael T. McGinley – April 2, 2014

In 2013, reported data breaches reached an all-time high—at least 740 million records were compromised. Press Release, Online Trust Alliance (OTA), Online Trust Alliance Finds Data Breaches Spiked to Record Level in 2013; 89 Percent Could Have Been Prevented (Jan. 22, 2014). Businesses understandably are concerned because these breaches can be enormously costly. In 2012, for example, the average total organizational cost of a data breach to a U.S. company was over $5.4 million. Ponemon Inst., *2013 Cost of Data Breach Study: Global Analysis* 5 (May 2013). Recent events illustrate that for large companies experiencing a major data breach, the loss may be much greater. According to the OTA, 40 percent of the largest data breaches to date occurred in 2013. OTA, *2014 Data Protection & Breach Readiness Guide* 4 (Jan. 22, 2014). The recent data breach at Target Corp. offers a stark example: Some analysts estimate that Target's breach may end up costing the company close to $1 billion.Smaller firms fare no better against breaches and have less ability to absorb losses. The cyber-security forecast for U.S. businesses is dark.

While no amount of planning or employee training can eliminate entirely the risk of a data breach, there are six steps businesses can take prior to a breach occurring that may lower the risk of loss significantly.

1. Take Tech to the Top

A culture of cyber-security must start in the boardroom and C-suite. Gone are the days when cyber-security was a topic understood and appreciated only by a company's "techies" in the information-technology department. Too much is at stake. Senior executives need to be able to weigh intelligently the cyber-security risks facing their companies and to allocate resources appropriately. Executive-level cyber-security ignorance or inaction impedes a company's ability to prepare for and respond to a data breach by removing resources that would otherwise allow the company to plan, recruit, and budget in a way that minimizes cyber-security risk.

Recent research suggests that both chief executives and members of the board need to improve their understanding of cyber-risk. For example, corporate boards do not appear confident that their chief executives understand the cyber-threats their own companies face—only 49 percent of surveyed directors felt that their CEO had a strong understanding of cyber-security. EisnerAmper, *Concerns About Risks Confronting Boards, Fourth Annual Board of Directors Survey* 16 (2013). Research data suggest that board members, too, lack a sufficient understanding of cyber-security risk. A 2012 Carnegie Mellon CyLab study found that 81 percent of North American boards rarely or never review annual budgets for privacy and information-technology security programs; 67 percent rarely or never review and approve roles and responsibilities of personnel responsible for privacy and security risks; 56 percent rarely or never review top-level privacy and security-risk policies, and 37 percent rarely or never review security-program assessments. Jody Westby, *Governance of Enterprise Security: CyLab 2012 Report; How Boards & Senior Executives Are Managing Cyber Risks* 17 (Carnegie Mellon Univ. CyLab May

16, 2012). And the survey revealed that nearly one-quarter of board members rarely or never receive reports on security breaches or loss of data.

Given these statistics, it is perhaps unsurprising that many large companies do not follow cyber-security best practices for staffing. The CyLab study found that less than two-thirds of companies in the Forbes Global 2000 list follow internationally accepted best practices, by failing to have full-time personnel in key roles responsible for privacy and security. *Id.* at 21. This can be costly. For example, appointment of a computer information security officer (CISO) with responsibility for enterprise-level data management and security can reduce the cost of a data breach dramatically. The 2013 Ponemon study showed that CISO appointment is one of the most effective methods of reducing the cost of a data breach, after creation of a strong security posture and implementation of an incident response plan. Ponemon Inst., *2013 Cost of Data Breach Study*, *supra*, at 9.

2. Adopt a Defensive Security Posture

Although the cost of a cyber-attack can be staggering, a company with a security posture may be able to reduce the cost of an attack significantly. A study analyzing 500 breaches in 2013 indicated that 89 percent of the breaches could have been prevented if the affected company had implemented simple security controls and best practices. OTA, *2014 Data Protection & Breach Readiness Guide*, *supra*, at 8. In fact, a U.S. business with a strong security posture can reduce the cost of a breach by up to $34 per record. Ponemon Inst., *2013 Cost of Data Breach Study*, *supra*, at 10.

At a minimum, companies should be keeping their antivirus and anti-malware programs up-to-date and be staying current with regularly released vendor software patches. Companies also should implement administrative controls (e.g., proper training), technical controls (e.g., forcing complex passwords), and physical controls (e.g., gates, physically locked doors to server areas or unsecured computers). Businesses also should review the SANS 20 Critical Controls, an excellent source of cyber-security best practices to protect against real-world threats.

3. Create a Data-Management Plan

A good data-management plan is an invaluable tool for preventing the loss of sensitive data in the first instance. The moment that a breach of sensitive data is detected is not the time to discover that your company unwittingly kept the data on its servers despite no longer having a business need for it.

A data-management plan helps to prevent such error. A data-management plan documents the collection, use, retention, transfer, and disposal of a company's data. At the most basic level, a data-management plan should be designed to ensure compliance with applicable state and federal laws (for example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm-Leach-Bliley Act). The plan should limit the sensitive data a company collects to the data that are absolutely necessary and should ensure that data collection and use align with the company's posted privacy policy. Collection of sensitive data creates liability, and the data-

management plan should consider the business purpose of all information the business plans to collect. The plan also should identify where the data will be used, to include identification of laptops, mobile devices, and cloud-based servers where users will access and modify the data. A data-management plan also should document how such data will be used. Importantly, users should have access only to those data they need to perform their jobs. The plan also should identify how employees will transfer data. This will help identify the correct level of security, which becomes more difficult as devices allow greater levels of mobile access. Next, the data-management plan should cover data retention, including where the data will reside. This issue is of particular importance if a company stores sensitive data of U.S. citizens overseas. The plan also should identify vendor access to sensitive information and require vendors to show their compliance with the company's data-security policies. Failure to ensure that vendors are practicing data security creates litigation risk and creates the perception that the company is being careless with customer data.

And, critically, a data-management plan should cover data disposal. Today's technology has drastically reduced the cost of technology required to store data, making it tempting to simply retain everything. This is a bad idea. The message here is simple: You can't lose what you don't have, so don't keep what you don't need. An annual audit is one way to reduce unnecessary sensitive data on a regular basis.

4. Create an Incident-Response Plan

Despite your client's best efforts, a breach likely will occur. In the chaos that inevitably ensues following realization that a company's sensitive data have been compromised, having an incident-response plan already in place greatly facilitates a comprehensive, orderly, and legally defensible response. This is not the time to improvise. A business with an incident-response plan in place when a data breach occurs can expect to reduce the cost of the breach by as much as $42 per record. Ponemon Inst., *2013 Cost of Data Breach Study*, *supra*, at 10.

An incident-response plan should identify internal-response-team members and provide general technical guidance for containing a breach without ruining legal evidence. Evidence may become inadmissible if data are modified or the chain of custody disrupted. An incident-response plan should ensure that the chain of custody for evidence is maintained and tracked properly (who collects it, who transfers it, and where it is stored). Further, a company should anticipate that if it hires a forensics firm to investigate a breach, any reports the forensics firm generates will be subpoenaed. To maintain privilege on these reports, companies should have legal counsel hire the forensics team and request forensics reports. And the incident-response plan should instruct that a litigation hold should be considered on a case-by-case basis and provide the procedures to be followed in such instances.

An incident-response plan also should articulate both internal and external notification requirements. External notification requirements may be particularly complex because notification requirements vary by country, state, industry, and type of breach. Best practice is to use the most stringent requirement from the assortment of applicable state laws. The OTA

recommends drafting a template that meets the requirements of most states where notification would be applicable, then adding one or more additional templates to address states with additional or conflicting requirements. OTA, *2014 Data Protection & Breach Readiness Guide*, *supra*,at 18. Keep in mind that the timing of the notification may be dependent on a government investigation, and that in addition to notification requirements to federal and state government regulators and law enforcement, contractual requirements may require notification to vendors and suppliers. And consideration also should be given to how the breach will be communicated to those whose records have been lost—for example, via email, regular mail, or the company's website.

Finally, it is worthwhile to keep an eye on whether Congress enacts any one of the proposed data-breach-notification bills that have been introduced this congressional session. Some of these bill provisions warrant particular attention because they would create criminal liability for failing to report a data breach. For example, the Personal Data Protection and Breach Accountability Act of 2014, introduced by Senator Richard Blumenthal (D-CT) and Senator Ed Markey (D-MA) on February 4, 2014, includes the following passage:

Whoever, having knowledge of a security breach and of the fact that notice of such security breach is required under title II of the Personal Data Protection and Breach Accountability Act of 2014, intentionally or willfully conceals the fact of such security breach and which breach, shall, in the event that such security breach results in economic harm or substantial emotional distress to 1 or more persons, shall be fined under this title or imprisoned not more than 5 years, or both.

Sen. Patrick Leahy, Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. § 1041 (2014). An identical bill, Personal Data Privacy and Security Act of 2014, H.R. 3990, 113th Cong. § 1041 (2014), and Senator Jay Rockefeller, Data Security and Breach Notification Act of 2014, S. 1976, 113th Cong. § 1041 (2014), have put forth similar proposals that do not impose criminal penalties unless economic damage exceeds $1,000.

While some of these provisions have been introduced previously without success, this Congress is pursuing data-breach legislation with zeal, so companies should a keep close watch on developments and update their incident-response plans as needed.

5. Establish and Train an Incident-Response Team

The incident-response plan is of no use without personnel trained and ready to execute the plan. The National Institute of Standards and Technology (NIST) has published guidelines for establishing incident-response teams and handling incidents. *See* NIST Spec. Publ. 800-61, Revision 2 (Aug. 2012). The incident-response team should be led by a senior executive, preferably a member of the board or a senior corporate officer. The team should consist of management plus staff of all of the functional components of the business because a breach of sensitive corporate information quickly can envelop every one of a company's functions. Accordingly, and depending on the size and structure of the business, the incident-response team should include representation from the following departments: information security, information

technology, risk management, human resources, operations, legal, public relations, marketing, finance, customer service, sales, business development, procurement, and investor relations. All of a company's employees should be aware of the incident-response team's existence and its role in a breach.

Critically, companies must ensure their incident-response teams are trained properly. Regular tabletop-style exercises offer response-team members the opportunity to envision and respond to applicable threats and to build relationships with other members of the team. These exercises will benefit particularly those executives who will interface with the press. Because stonewalling the press is not a good idea, the team should anticipate questions about the breach and be prepared to provide the press some basic information. For larger companies, the incident-response team should be prepared to direct the opening of a call center following a major breach. Call centers may do more harm than good if call-center employees lack proper guidance. Accordingly, the response team should create a call-center script and train call-center employees not to go off the script.

6. Develop External Relationships

A data breach is a multidisciplinary event. A proper response requires the involvement of many players, many of whom are external to the breached company. To that end, building strong relationships with external organizations is a must. Developing trust with law enforcement and regulatory entities (for example, local FBI agents or attorneys in a state's office of the attorney general) may pay dividends when a breach occurs and the breached company's version of events comes under scrutiny. And law enforcement and regulators prefer to receive bad news directly from your client—not cyber-security blogger Brian Krebs.

Supplier relationships also are important. The interconnected nature of business means that a breach at one business is likely to affect the operations of connected businesses. In addition, a company should have a working relationship with those vendors to which the company will turn in the event of a breach (such as external legal counsel, forensics, and identity-theft-management companies, call centers, and credit-monitoring services). Businesses should engage data-breach service providers prior to a breach and put in place nondisclosure and service agreements to facilitate vendor response following discovery of a data breach. A word of caution, however: A company's insurer often determines which vendors the insured company must use in the event of a data breach.

Keywords: criminal litigation, data breach, cyber-security, cyber-attack, response plan, data management

Michael T. McGinley is an associate with Wiggin and Dana LLP in Stamford, Connecticut.