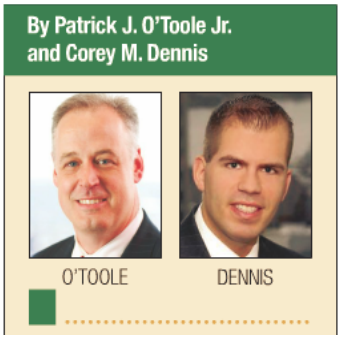
New England IN-HOUSE

Best practices for avoiding data breach liability

August 2013



Data breaches and cyber-attacks are an unfortunate reality. In the past few years, Google, Yahoo, LinkedIn, and Wyndham Hotels have all faced data security breaches. Now, security breaches are an increasing threat to all businesses. In May, Yahoo Japan notified users that a breach may have compromised 22 million user IDs, and in late April, LivingSocial, an online daily deal website, notified more than 50 million customers of a breach resulting from a cyber-attack.

The risk of liability and reputational damage associated with such incidents has escalated, and many key industries—including defense, financial services, health care, retail, pharmaceutical and energy—are the intended targets. Even more troubling is that the threat is often hidden, with companies not knowing that they have been hacked or that valuable information, including trade secrets or other intellectual property, has been stolen until after significant damage has occurred.

Moreover, a data security incident involving lost or stolen personal information of customers or employees—whether resulting from malicious hacking or employee negligence—may lead to enforcement actions from increasingly active state and federal regulators, fines for failure to comply with payment card data security standards, major news headlines, and even consumer class action lawsuits. It is not surprising, then, that data security is now a top concern for both general counsel and corporate directors.

The data privacy and security regulatory scheme has become more complex in recent years, making it challenging for companies to comply, particularly those in highly regulated industries, such as health care. In fact, the U.S. Department of Health and Human Services Office of Civil Rights' recent HIPAA audit pilot program revealed that many health care organizations are not even aware of applicable requirements. HHS received over 78,000 breach reports from September 2009 to March 2013, and imposed nearly $15 million in HIPAA non-compliance penalties from 2008 to 2012.

Data breach prevention

Companies should take the following precautions to minimize the likelihood of a data breach and potential liability:

- **Identify all sensitive data handled by the company, its custodians and its storage locations.** Conducting an inventory of your company's sensitive data is an essential step in safeguarding that information.

- **Ensure compliance with state and federal regulatory requirements.** Depending on the type of data your company holds, it may be subject to a broad array of state and federal laws, including HIPAA, the Gramm-Leach-Bliley Act and state data security regulations. Consult with legal counsel to ensure compliance with the complex patchwork of laws.

- **Regularly review and update your company's written information security policies.** This is a requirement under some federal and state laws and a recommended practice for all companies.

- **Implement and maintain both computer system security measures and physical security measures.** While computer security measures (e.g., passwords, encryption, firewalls, anti-virus software) are critical, physical security measures (e.g., locked cabinets, shredders) are equally important to safeguarding sensitive data and personal information. Some state laws, including the Massachusetts data security regulations, require that businesses encrypt personal information stored on portable devices or transmitted wirelessly. Nonetheless, encryption is a recommended best practice for all companies.

- **Implement best practices and train employees.** A company's policies are only as good as its practices. Many data breaches result not from sophisticated cyber-attacks, but from basic employee negligence, such as the loss of a laptop or paper records containing sensitive information. For example, Massachusetts General Hospital was fined $1 million in 2011 after an employee left documents containing sensitive information on the subway. Conduct periodic training sessions to ensure that all employees understand and comply with the company's information security policies.

- **Ensure vendor compliance.** Exercise diligence when retaining third-party service providers or "business associates" with whom sensitive information may be shared. In some circumstances, a company may be found liable for its vendor's non-compliance. Under some federal and state laws, including the Massachusetts data security regulations, companies must require their vendors by contract to maintain certain data security measures.

- **Conduct periodic attorney-directed data security assessments.** Such assessments will assist in detecting vulnerabilities and ensuring compliance with applicable laws. Businesses should retain outside counsel in order to preserve the attorney-client privilege applicable to any reports or other communications relating to the assessment.

- **Consider cyber liability insurance.** Companies have had only mixed success in relying on traditional insurance policies to cover the costs associated with data breaches. Many companies now purchase cyber liability insurance, which is specifically designed to cover the costs of forensic investigations, notification and credit monitoring for affected individuals, regulatory compliance, defending lawsuits, and payment of any resulting judgments or settlements.

Responding to a data breach

Although the steps outlined above will reduce the risk of a data breach, not all breaches are avoidable. In the event of a data breach, companies must comply with data breach notification laws, which have been enacted in 46 states and the District of Columbia.

Although data breach notification laws vary by jurisdiction, generally businesses must notify consumers whose personal information has been compromised by a security breach—and in many states, the attorney general or other state agencies—"in the most expedient time possible" or "without unreasonable delay." *See, e.g.,* Cal. Civ. Code § 1798.82; Mass. Gen. Laws ch. 93H, § 3; N.Y. Gen. Bus. § 899-aa; R.I. Gen. Laws 11-49.2-3.

However, some states impose more stringent notification deadlines. For example, Vermont and Florida require notification within 45 days, while California has a five-day notification requirement for hospitals and nursing facilities.

At the federal level, the HITECH Act's breach notification rules require health care organizations to report data breaches involving 500 or more individuals to the affected individuals, the U.S. Department of Health and Human Services, and "prominent media outlets serving a State or jurisdiction" within 60 days. Breaches involving fewer than 500 individuals must be reported to the department annually.

Data breaches become a crisis situation for many companies, with management scrambling to determine what happened, how it happened, and what steps to take to mitigate the damage. To limit potential liability for a data breach, companies should:

- **Maintain an incident-response plan and team.** The incident-response plan, prepared before an incident occurs, should identify the team members (e.g., executive management, IT, legal, human resources and public relations professionals), specify each team member's responsibilities, outline breach response measures, and involve outside professionals (i.e., legal, forensic, public relations) immediately following an incident.

- **Remember that time is of the essence.** It is important to act quickly when facing a data security incident, given the deadlines under applicable state and federal laws. Failure to do so could lead to both increased regulatory scrutiny and liability.

- **Consult with legal counsel.** Data breaches are often complex and may affect thousands, or even millions, of individuals, necessitating compliance with dozens of breach notification statutes. It is recommended that outside counsel be consulted to guide the breach response, ensure compliance, and preserve applicable privileges. When dealing with complex breaches, engaging an outside forensics investigation firm may also be recommended.

- **Preserve corporate reputation.** Large breaches make the headlines. It is critical for the company to preserve its reputation with both the affected individuals and the general public. Engaging a public relations firm may be helpful in this regard. Offering credit monitoring to affected individuals may also help to maintain corporate reputation,

reduce the risk of consumer identity theft and potential lawsuits, and appease regulators.

In the digital age, cyber-attacks and data breaches are constant threats to businesses. With breaches of large, sophisticated companies coming to light nearly every day, and state and federal regulators taking a hard line approach to data security, businesses are understandably concerned.

To combat this increasing threat, companies should implement best practices to minimize the risk of a data breach and resulting liability. Prevention and self-protection are essential components to reduce the threat and impact of data breaches and cyber-attacks.

Patrick J. O'Toole Jr. is a partner at Weil, Gotshal & Manges in Boston. He practices in the firm's complex litigation group and white-collar defense and investigation practice. Corey M. Dennis, an associate at Governo Law Firm in Boston, represents companies in complex litigation and counsels them on compliance with privacy and data security laws.