Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Practical Lessons From Recent Data Breaches

Law360, New York (July 09, 2012, 2:31 PM ET) -- Recent data breaches at popular Internet sites, including the theft of millions of user passwords by hackers at business networking site LinkedIn and dating site eHarmony, are a timely reminder of the substantial financial and other consequences businesses potentially face from unauthorized access to private data.

Although the exact costs for large breaches such as the theft of the 8 million LinkedIn and eHarmony passwords, allegedly obtained by Russian hackers, are difficult to determine, a recent study estimates that the average cost of breaches involving less than 100,000 records is $194 per capita, including costs of detecting and reporting the breach, notifying and assisting consumers, and opportunity costs such as turnover of existing customers. Not included in this estimate are the substantial legal costs required to defend class actions that are almost inevitable consequences of a major data breach and the nonmonetary harm to reputation and goodwill. Indeed, LinkedIn was hit with a class action a little more than a week after the breach was reported.

In light of the numerous adverse effects stemming from a data breach, businesses should consider taking practical steps to assess their vulnerabilities and to protect themselves from unauthorized access by hackers and others.

1) Implement Appropriate and Reasonable Security Measures

The first and most basic step a business can take is to make an assessment of its security measures in light of security requirements and the data collected by the business to determine if they are adequate to protect crucial data, including customer and consumer records and trade secrets. Such risk assessments, which should include protecting data from unauthorized access, are a crucial part of any security program.

Indeed, research indicates that 97 percent of breaches were avoidable through simple or intermediate controls. Underscoring the importance of implementing basic protections are the adverse consequences that could be caused by news reports revealing that a company has failed to implement basic protections, such as firewalls, patches to security programs, or, as with the recent breach of LinkedIn, commonly used protection techniques for user passwords.

Having adequate measures in place for data security is not only a good business practice, it is often required by law. Depending upon industry sector, businesses may be required to comply with the specific data security requirements of federal regulatory authorities, including the Federal Trade Commission and the U.S. Department of Health and Human Services, as well as those of many states and foreign countries. Moreover, the FTC is increasingly active in bringing actions against companies with inadequate data security practices under the authority granted by Section 5 of the Federal Trade Commission Act prohibiting "unfair" and "deceptive" acts and practices.

2) Understand Data Breach Reporting Requirements Before a Breach Occurs

If a data breach includes unauthorized access to certain sensitive or private categories of information, such as Social Security numbers or protected health information, a business may be promptly required to report the breach to the persons affected and, in some instances, to state or regulatory authorities. For example, an entity conducting business in California is required to notify California residents if "unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person" in "the most expedient time possible and without unreasonable delay" regardless of whether there is any likelihood of harm from the breach. Civil Code § 1798.82 et seq.

If the breach involves more than 500 California residents, the business is also required to notify the California attorney general. Companies conducting business in Arizona are required to provide notice to an individual, "in the most expedient manner possible" when the company learns of "an incident of unauthorized acquisition and access to unencrypted and unredacted data that includes [the] individual's personal information." Ariz. Rev. Stat. Ann. §44-7501(A).

Other states, including Texas and Massachusetts, have broad data security rules that apply to any entity, wherever located, that holds personal information regarding the state's residents. See Mass. Gen. Laws ch. 93H-1 et seq.; Tex. Bus. & Com. Code § 521.03, Tex. Ed. Code 37.007(b)(5) (2011 H.B. 1224). Indeed, after Sept. 1, 2012, Texas will require businesses who conduct business in the state to provide notice not only to Texas residents, but "to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Tex. Bus. & Com. Code § 521.03(b) (effective Sept. 1, 2012).

Depending upon industry sector and the type of data involved, a business may also be required to provide notification of breaches under federal laws such as the Health Insurance Portability and Accountability Act, the Health Insurance Technology for Economic and Clinical Health Act and the Gramm-Leach-Bliley Act.

Complying with the myriad of data breach notification requirements imposed by the states and the federal government is undoubtedly challenging and potentially expensive.

Over recent years, numerous proposals for a national data breach law have been introduced into Congress, without success. Although these bills differ in significant details, they would generally preempt state data breach notification laws. The most recent of such bills, which was introduced on June 22, 2012 by Sen. Pat Toomey, R-Pa., would require notice to U.S. citizens or residents if an entity "reasonably believes" an individual's personal information has been "accessed and acquired by an unauthorized person" and that such information "has caused or will cause, identity theft or other financial harm." See Data Security and Breach Notification Act of 2012, S. 3333, 112th Cong. § 3(a)(1). Sen. Toomey's bill explicitly prohibits private causes of action for violations of the act. Id. § 4(d).

In its February 2012 proposal for a consumer privacy bill of rights, the White House also proposed a national standard for notification of security breaches noting that the current "patchwork of State laws" imposes "significant burdens." See Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, p. 39. Given the complexities of the current landscape, it is advisable for businesses not only to perform an assessment of the security and data breach laws to which they are subject, but also to have procedures in place to notify consumers and government authorities as required by applicable law and regulation in the event a breach occurs.

3) Incorporate Privacy by Design Principles Into All Aspects of Operations

Because security breaches frequently involve personal or sensitive information regarding customers, consumers and employees, businesses should also be proactive in protecting data security and privacy at all stages of their systems and processes. These protections — which are increasingly being adopted by businesses under the rubric of "privacy by design" — treat privacy and data security as a default built into the process or system, rather than an afterthought. Adopting privacy by design is advisable not only for risk management purposes, but also because it may be required by future law.

In its March 2012 report "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," the FTC urged companies to embrace privacy by design "throughout their organizations and at every stage of the development of their products and services." The FTC also called on companies "to incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy." Similarly, the European Union's proposed data protection regulation would require data protection by design and default. Companies that implement privacy by design principles, including data security, may gain a head start on what could become legal requirements in the United States and other jurisdictions.

Although the details of compliance with data security requirements vary from jurisdiction to jurisdiction, as well as by business sector, adherence to the practical steps outlined above may allow businesses to avoid some of the risk from what is unfortunately becoming part of the normal landscape of an interconnected world.

--By Timothy J. Toohey, Snell & Wilmer LLP

Timothy Toohey is a partner in Snell & Wilmer's Los Angeles office.

The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.