Schnader
ATTORNEYS AT LAW

Schnader Harrison Segal & Lewis LLP

NEW YORK PENNSYLVANIA CALIFORNIA WASHINGTON, D.C. NEW JERSEY DELAWARE

E-COMMERCE & TECHNOLOGY
ALERT

MAY
2013

Data Breach — Your Organization Needs a Plan

By Nicole Reimann

The Privacy Rights Clearinghouse's Chronology of Data Breaches lists 3,671 incidents affecting 607,295,463 records since 2005,[1] including these three:

- A worker steals customer records containing credit card, bank account and other personal information. In its U.S. Securities and Exchange Commission filing, the company estimates that 8.5 million records are affected.
- A password-protected laptop containing former employee names, Social Security numbers, birthdates, and benefits information is stolen from a consultant's trunk with an estimated 5,800 records affected.
- Cyber-pickpockets tamper with PIN pads in retail stores and steal banking information from checkout keypads. Ninety-four thousand records are affected.

Taking steps to protect personal information can go a long way to preventing a security breach. No technology is fail-safe, however.

Today most companies come in contact with or store personal information. This is not only the domain of large organizations, relatively small ones face potential liability should personal information be compromised in a security breach of the organization's computer systems. The potential for disclosure of personal information exposes all organizations to potential liability for damages and the cost of breach notification and remediation.

The most recent Ponemon Institute Cost of Data Breach Study reports that whether the result of lost laptops, misplaced thumb drives, malicious software, or system glitches, data breaches carry very serious financial consequences — costing on average a breathtaking $5.5 million per data breach — or $194 in direct and indirect costs per record compromised.[2] Forensic experts, outsourcing hotline support, free credit monitoring subscriptions and discounts for future products and services account for one-third of the $194 per record cost of a data breach. Loss of reputation, damage to brand, and the cost of in-house investigation and communication account for the other two-thirds. Senior level managers estimate that it can take a year to restore an organization's reputation after a data breach involving 100,000 customer records that is reported widely in the media.[3]

To manage reputation, contain costs and business disruption, and stay within the law, your organization needs a plan. Four factors drive up the cost of a data breach: inexperience, involvement of third party providers, data breaches involving mobile devices, and quick notification of breach victims.[4]

Organizations responding to and remediating their first data breach spend $37 more per record than those who have dealt with a data breach before. Experience sharpens intuition. It also drives home the need for a response plan. Do you have a written response plan?

Data breaches caused by outsourcers, cloud providers or business partners cost $25 more per record than breaches with an "in-house" cause. Do your contracts with third parties address data breaches? Do they require them to comply with your data security standard?

(continued on page 2)

1. A chronology of data breaches is available at Chronology of Data Breaches, Privacy Rights Clearinghouse, http://www.privacyrights.org/data-breach (last accessed May 5, 2013).
2. Ponemon Institute LLC, 2011 Cost of Data Breach Study: United States (March 2012).
3. Ponemon Institute LLC, "Reputation Impact of a Data Breach" (October 2012).
4. Ponemon Institute LLC, "2011 Cost of Data Breach Study: United States" at pp. 8-10 www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf .

(continued from page 1)

A data breach involving lost or stolen mobile devices, such as laptops, smartphones, tablets and USB drives, costs $23 more per record than breaches involving other hardware. Are your mobile devices encrypted?

Notifying victims quickly increases costs by $32 per record. Timing of notice needs to comply with applicable law. Moving too quickly, that is before you have adequate information for meaningful notification, however will likely be more costly to the organization and less helpful to the breach victim. Will you have privacy counsel to advise you on the legal notification requirements for breach victims and others?

What are the attributes of organizations whose direct and indirect costs for a data breach fall below the average? They designate an information security leader with organization-wide responsibility, and they hire external experts to assist with response and remediation, saving $79 and $41 respectively per record compromised.[5]

The results of the Ponemon Institute Cost of Data Breach Study underscore the observations of every expert on privacy compliance and data security — an organization needs to be prepared. Designate a response team. Inventory and classify data. Educate employees about privacy issues. Prepare a "what if?" action plan. Your business, your customers and your employees will benefit.

Designate a Team

Set the tone for the organization's commitment to data security. Your team may look different from other organizations, but begin by designating a well-respected senior official who has a track record of working well with every part of the organization, and give this person a hotline to the head of the company. A team should also typically include inside members from legal, communications, information technology, human resources and compliance. Outside members should include outside counsel, public relations, electronic forensics consultants and law enforcement. Keep contact information for team members current so that team members can be contacted quickly when necessary.

5. Id. at p. 10.

Inventory, Classify and Educate

- Inventory records systems, computing systems and storage media containing personal information.
- Classify personal information according to sensitivity.
- Conduct ongoing employee training to promote awareness of security and privacy policies.
- Require service providers and business partners who handle personal information to follow your security policies.

Make a Plan

Draft contingency plans for how your organization will respond to different security incidents. Some threats come out of left field; others such as a lost thumb drive or malicious attack — are foreseeable. Among the practices and information that should be included in a response plan are:

- Written procedure for identifying a breach incident that warrants activating the response team.
- Written procedures for internal notification of security incidents that may involve unauthorized access to sensitive personal information.
- Measures to control, contain and correct a security incident.
- Ongoing training of employees in their role and responsibilities in the response plan.
- Immediate notification by data custodians of detected security incident.
- Identification of law enforcement contacts for security incidents that may involve illegal activity.
- Identification of government agencies you are required to notify of a breach.
- Prior consent to notify affected individuals by email if such consent is required.
- Protocol for documenting response to security incident.
- Written procedures for notification of individuals to the extent required by applicable law.

(continued on page 3)

(continued from page 2)

Your Organization Suspects a Data Breach — What Now?

If employees suspect a security breach, investigate it immediately. Containment — stopping the access to or distribution of personal information — is the first priority. A computer forensic expert can assist in determining whether personal information was involved in the data breach and identify the affected persons. Meanwhile, legal counsel should address potential regulatory violations, ensure that evidence is preserved for use in court or an agency investigation, consider liability of third party providers and determine whether breach notification is required and how notice will be accomplished, including timing, content and method of notice.

Breach notification statutes have been criticized for creating "a fragmented, incoherent liability scheme."[6] Federal statutes that focus on particular economic sectors such as healthcare and financial services, including the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH) and the Gramm-Leach-Bliley Act (GLBA), require notification under certain circumstances. In addition, 46 states have enacted breach notification laws. State breach notification laws cause compliance challenges for organizations engaged in interstate commerce. Variations in state security breach notification law have been described as "so numerous that it is virtually impossible to convert these state laws into the more manageable format of fifty-state surveys."[7] Consult with legal counsel before you decide:

- With whom to communicate?
- What to communicate?
- How to communicate?
- When to communicate?

◆

For more information about Schnader's E-Commerce and Technology Practice Group or to speak with a member of the Firm, please contact:

Ronald E. Karam, Co-Chair
215-751-2364
rkaram@schnader.com

Theresa E. Loscalzo, Co-Chair
215-751-2254
tloscalzo@schnader.com

Nicole Reimann
215-751-2295
nreimann@schnader.com

6. Winn, Jane K., "Are 'Better' Security Breach Notification Laws Possible?" 23 (June 8, 2009) *Berkley Technology Law Journal*, Vol. 24, 2009. Available at SSRN: http://ssrn.com/abstract=1416222.

7. Tom, Jacqueline May, "A Simple Compromise: The Need for a Federal Data Breach Notification Law," 84 *St. John's Law Review* 1569 (2010).