Risk Management: Cyber Insurance & Your Data Breach Response Plan

By:
Theodore J. Kobus III, Esq.
and Kimberly M. Wong, Esq.
About the Authors:

**Theodore J. Kobus III, Esq.**, is a partner and National Co-Leader of the Privacy, Security & Social Media Team at Baker & Hostetler, LLP. Ted has an extensive background advising clients, trade groups and organizations on data security and privacy risk management, breaches, response strategies, litigation and regulatory actions affecting organizations. He has counseled clients involved in significant breaches implicating state and federal laws, international laws and other regulations and requirements, and has dealt with Offices of Attorneys General, state insurance departments, Office of Civil Rights (OCR)/Health and Human Services (HHS), Secret Service, FBI and local police and forensics professionals as part of their handling of data breaches. Ted has handled more than 300 breaches and his experience extends to litigation of data breaches, privacy, technology, media and intellectual property matters. Questions regarding privacy and data security can be directed to tkobus@bakerlaw.com or 212-271-1504.

**Kimberly M. Wong, Esq.**, is an associate at Baker & Hostetler, LLP. Kimberly focuses her practice in the areas of intellectual property, privacy, data breach and social media. She advises corporations, healthcare providers and other entities on compliance with state and federal data breach notification laws and identity theft regulations. This includes counseling with respect to responding to breaches of sensitive personal information and/or protected health information, establishing written information security programs, crafting identity theft prevention programs pursuant to the FTC’s Red Flag Rules and maintaining the security of personal health information pursuant to HIPAA and HITECH. Kimberly has also advised clients on regulatory investigations arising from data breaches, including investigations by the U.S. Department of Health & Human Services, the U.S. Department of Education and various State Attorneys General. Kimberly can be reached at kwong@bakerlaw.com or 212-271-2028.

**Legal Notice:** The information you obtain herein is not, nor intended to be, legal advice. We try to provide quality information but make no claims, promises or guarantees about the accuracy, completeness or adequacy of the information contained. As legal advice must be tailored to the specific circumstances of each case and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent legal counsel.
In recent months, several entities have publicly announced being affected by a cyber incident. Almost daily, online accounts are hacked, external hard drives are stolen, thumb drives are lost and backup tapes are trashed. In all of these instances, personal information is at risk of being accessed and misused. Cyber incidents happen, from the simple mistake of misplacing an external hard drive containing protected health information, to the more complex instance of malware intrusion into a financial institution’s customer accounts.

In 2010, of 2,100 hundred companies participating in a survey, 73% of small and midsized businesses reported experiencing a cyber incident in the last year.\(^1\) Since January 2005, the total number of records containing sensitive personal information involved in security breaches in the U.S. is more than 562 million, which relates to 3,136 data breaches.\(^2\) A simple mistake, or a more sophisticated event, can cause a cyber incident resulting in a multitude of issues for an entity.

In the Ponemon Institute’s Cost of a Data Breach Report for 2011, a survey of 49 U.S. companies in 14 different industry sectors, 39% of organizations stated negligence was the root cause of a data breach.\(^3\) Also, when a cyber incident affects an entity for the first time, various issues are compounded by the stress of the unfamiliar. When a cyber incident occurs, first and foremost, how do you protect your customers? Second, how do you protect your business?

Immediately upon discovery of a cyber incident, the following questions usually arise:

- What happened?
- What data was affected?
- How many individuals were affected?
- Should we notify affected individuals immediately?
- Do we have a legal obligation to notify?
- Whom do we notify? Business partners? Law Enforcement or regulatory agencies?

These questions may seem elementary, but the answers can be challenging and often lead to additional questions:

- Should we engage forensic investigators to determine what data was affected and whether the data was actually accessed or misused?
- Should we hire crisis management professionals to assist with PR?
- Should we engage legal counsel to assist in determining federal and state notification obligations?
- Should we hire vendors to assist with any notifications, even if voluntarily notifying?
- Should we employ a call center service to assist with questions from customers?
- Should we offer credit monitoring to affected individuals?
- Is it likely that a regulatory investigation will follow or that a lawsuit will be filed?

---

1 2010 Global SMB Information Protection Study
3 Cost of a Data Breach Report for 2011, Ponemon Institute, March 2012.
Notification expenses are often covered, perhaps even when no legal obligation is triggered to notify affected individuals.

**Cyber insurance basics**

Cyber insurance not only helps organizations to respond to these questions, but the experience the carriers have gained through responding to claims will help an organization better position itself to respond to a data security event.

Cyber insurance policies continue to evolve as laws change and new claims arise. Policies can be customized in order to address any cyber-related incident that pertains to an entity’s data. In order to protect an entity from a cyber incident, a cyber insurance policy should provide third-party coverage (“cyber liability”) that covers (1) losses resulting from breaches in network security or events pertaining to unauthorized access (network security and privacy coverage) and (2) costs resulting from a civil, administrative or regulatory proceeding that alleges a violation of a privacy law (privacy regulatory proceeding coverage).

First-party coverage is also available to provide against losses such as data destruction, extortion, theft, hacking, loss of revenue caused by interests to data flow or network systems. Notification expenses (including printing and mailing, call center support, credit monitoring, forensics, legal counsel and crisis management expenses) are often covered as well, perhaps even when no legal obligation is triggered to notify individuals affected by a data security incident.

**Things to discuss with your broker**

Determine what coverage currently exists under general liability and/or professional liability policies. This determination begins with a discussion regarding an entity’s exposure and type of policy necessary to minimize such exposure. Identify the types of cyber incidents that can affect your business. Do you store data in areas that are vulnerable to theft or other loss? Do you maintain Social Security numbers, credit card numbers, drivers’ license information, health information or bank account information? How many people does that information relate to? What type of network logs are in place to track access to the sensitive data you maintain?

Next, consider loss scenarios. This will help determine what may not be covered by a first-party insurance policy. Loss scenarios include employees/non-employees stealing data; hacking causing data exposure; employee/non-employee theft of computer equipment; publication of information on the Internet, etc. Even though you may have the proper cyber coverage to address these types of losses, consider implementing appropriate training programs for employees. Employee negligence is a major cause of data loss and training is one way to help reduce the frequency of these types of events.
Healthcare industry

Exposures in the healthcare industry are unique, particularly since the passing of the Health Information Technology for Economic and Clinical Health (HITECH) breach notification rule. As such, cyber insurance has been especially popular in the healthcare sector. The HITECH Act breach notification rule requires covered entities to report an impermissible use or disclosure of protected health information or a “breach” of 500 or more individuals to the Department of Health and Human Services (HHS) and the media. Smaller breaches that affect less than 500 individuals are reported annually to HHS.

HHS’s Office for Civil Rights (OCR) is responsible for enforcement of the Privacy and Security Rules under the Health Insurance Portability and Accountability Act (HIPAA) and investigates many breaches reported under HITECH. The Privacy Rule sets forth the standards to protect the privacy of patients’ medical records and other health information maintained by covered entities. The Security Rule sets forth a national standard for the security of electronic health information, providing a series of administrative, technical and physical procedures to assure confidentiality. Since enforcement of the Privacy Rule began in 2003, and continuing through the beginning of the enforcement of the Security Rule in 2009 by OCR, OCR has been proactive in investigating the privacy practices of covered entities, investigating and resolving more than 16,015 cases.

According to OCR, the two security-related compliance issues most investigated are: (1) impermissible uses and disclosures of protected health information and (2) lack of safeguards of protected health information. Recently, OCR entered into resolution agreements and issued civil monetary penalties associated with these issues.

On April 17, 2012, Phoenix Cardiac Surgery, P.C. agreed to pay HHS a $100,000 settlement and take corrective action to implement policies and procedures to safeguard the protected health information of its patients. Giving rise to OCR’s investigation was a report that the physician practice posted clinical appointments for its patients on an Internet-based calendar that was publicly accessible. The report led to further investigation as to the physician practice’s compliance with HIPAA Privacy and Security Rules. OCR found that the physician practice had insufficient safeguards in place to protect patients’ electronic protected health information.

Also noteworthy is the recent resolution of OCR’s first enforcement action resulting from a breach report required by HITECH. On March 9, 2012, Blue Cross Blue Shield of Tennessee (BCBST) agreed to pay $1.5 million to settle potential violations of the HIPAA Privacy and Security Rules, arising from BCBST’s notification to HHS that 57 unencrypted computer hard drives containing protected health information of more than 1 million patients had been stolen from a leased facility in Tennessee.
Annually, obtain an enterprise-wide network security risk assessment that analyzes the people, processes and technology underlying your security and privacy posture.

BCBST also agreed to take corrective action by reviewing, revising and maintaining its policies and procedures; providing additional training to all BCBST employees as to responsibilities under HIPAA; and performing monitor review to ensure BCBST compliance with the corrective action plan.

There are cyber insurance policies available not only to pay defense costs related to these types of regulatory matters, but also to pay the settlements in a resolution agreement with HHS.

**What to do now**

As personal data grows in value, the risk of a cyber event to any organization grows in value as well. Here are a few things you can do to improve your organization’s security and privacy posture – thereby reducing risk overall.

**Know the law**

Numerous privacy regulations and guidelines, i.e. FACTA, state data protection laws, HITECH, the Payment Card Industry Data Security Standard, Red Flag Rules, Safeguard Rules, require the protection of personally identifiable information regardless of where it resides. This includes data that is at rest, in transit, on a network, on a stand-alone system, on a remote device such as a laptop or a thumb drive and on paper. Identify the applicable laws and guidelines and determine how and where the laws and guidelines may impact your entity. Being legally compliant will help minimize the risk to your entity in the event of a cyber breach.

**Determine your exposure**

A first step in protecting your data is to determine what data exists and whether or not the data is needed. Superfluous data should not be collected. If the data is necessary, determine how to protect the information. Consider encryption. Conduct an internal, or an external third party, review of your computer system security. Also, determine how long the information is needed. Do you still have data from the ‘80s? It is likely that you do not need it. Once you have estimated your potential exposure, determine how to decrease your risk.

**Education and training are key components to any breach response preparation initiative**

Unfortunately, even the most compliant and security-focused organization can fall victim to a data breach. In fact, the most common cause of a cyber event today is not hacking, but simple human error. Data protection is not a one agency responsibility. Full compliance requires buy in by every employee. Most data breaches involve confidential information stored outside the network system on laptops, smartphones, thumb drives, etc. Educate your employees regarding your state’s statutes for protecting personal information. Train your employees on your entity’s policies and procedures for the safeguarding of personal information.
Understand your risks and vulnerabilities

Annually, obtain an enterprise-wide network security risk assessment that analyzes the people, processes and technology underlying your security and privacy posture. Allowing a third party to identify specific vulnerabilities and legal liabilities allows your entity to focus on the risks that need to be minimized. Considering the budgetary restraints that affect any entity, a risk assessment will help you focus funds where they are most needed.

Don't forget about business partners

Not only do you have an obligation to protect your entity’s data, you also have the obligation to employ business partners that also adequately protect personally identifiable information. Inquire as to your business partners’ policies and procedures for the safeguarding of personal information. Ask how their employees are trained regarding data protection. Most importantly, after completion of an engagement, verify with your business partner that all data is returned or destroyed.

Manage your risks

As discussed above, a cyber insurance policy may be a good idea, but remember that transferring your entity’s financial risk does not transfer your duty to implement and maintain appropriate safeguards for protecting information.

Be proactive in protecting your company’s name and public image; doing so will help protect your biggest asset – your customers. Know that a cyber event will happen – it is just a matter of time. Entities that have taken the appropriate measures before a cyber event occurs are better equipped to minimize the damage that may result. Review your policies and procedures for safeguarding personal information; train your employees regarding those policies and procedures. Determine where exposure exists and decrease the associated risks using some of the steps mentioned above. Your customers trust you with their personal information – ensure that their personal information is protected.

Entities that take the appropriate measures before a cyber event occurs are better equipped to minimize the damage that may result.

To learn more about data breach resolution, visit www.Experian.com/DataBreach or contact Experian® at databreachinfo@experian.com or 1 866 751 1323.