

“I Lost My Laptop. Now What?” – The Cost of a Data Breach

Consider this hypothetical situation: You finish your day at work and pack up your things to leave, taking your laptop with you so you can get some work done at home. On your way home, you stop by the grocery store. You make your purchases and return to the parking lot, and what you discover there makes your stomach turn over: Your car has been broken into.

When you look inside, you realize your laptop is missing. Your first thought is about how much that laptop will cost to be replaced. A thousand dollars? Maybe. But that's not the real cost of the theft. Your laptop contains personally identifiable information for your customers.

Your company has just experienced a data breach.

While most insurance professionals and insureds know there is insurance available to protect an organization facing this scenario, many still underestimate its value and the need for the product. The cost of replacing the laptop is inconsequential when compared to the exposure created by its loss. The data on the laptop is not covered by a property policy, and the liability from losing the data is also not a covered peril. A general liability policy would only provide coverage if there is bodily injury or property damage as a result of the loss of the laptop.

Severity of a Loss. The Ponemon Institute's "Cost of a Data Breach" study is published annually and illustrates how costly a breach can be. In the recently published edition, which summarizes the 2010 data, the study shows that the average data breach costs \$7.2 million, and the average expense per compromised record is \$214. The survey tracked expenses for data breaches ranging from 1,000 to 100,000 records. The least expensive breach cost a company \$780,000 and the most expensive was \$35.3 million. The average shown in the study does not include mega breaches such as Heartland Payment Systems (130 million records), TJX (94 million records) or TRW/Sears (90 million records), which would have pulled up the average dramatically. It is important to note within the study that \$141 of the \$214 per-record expense is made up of what the study calls "indirect costs," such as the loss of customers who stop doing business with the company after learning of the breach, and the costs associated with advertising and public relations efforts to repair the company's reputation. Notification, credit monitoring, forensics and other expenses make up the balance.

The potential expense from compromised data is large, but not as costly as pretending that it never happened and hoping no one figures it out. 46 out of 50 states have notification requirements following a data breach, and many have significant penalties based on the number of days a firm waits to report a data breach. For example, the State of Connecticut fined HealthNet \$250,000 because the company waited six months to report a data breach that impacted 1.5 million individuals. The breach was a result of the loss of a portable hard drive. It's important to note that the fines and penalties can be levied well in advance of the lost data actually causing harm. The mere potential exposure is enough to draw the attention of regulators. HealthNet, for example, was also ordered to establish a \$500,000 contingency fund in case the data was later found to be accessed and used against residents of Connecticut.

Legalities of a Loss. A firm will have an immediate expense when they have a data breach that triggers the notification requirements of the state where the victim resides (not necessarily where their business is domiciled). Different states have different reporting thresholds including a minimum number of records, perceived value of the lost data to identity thieves, and encryption level of lost data. Many states have vaguely defined requirements. To find state requirements, visit: http://datalossdb.org/us_states.

In addition to the state laws and regulations, there is a federal bill working its way through Congress that will provide some standardization to the notification requirements. The Federal Trade Commission already pushed out the Red Flag Rule, which requires businesses to have plans in place for prevention of and response to a data breach. (See our client advisory, [FTC Red Flag Rule Update](#), for more information.)

The HITECH Act also created more regulatory oversight of private health information and increased liability to health care providers' business associates. The Act defines "business associate" as anyone doing business with a health care provider and gives business associates the same level of liability as the health care organization if the business associate has contact with the personally identifiable information belonging to the health care organization. Firms providing services to health care organizations, including

To learn more about how AmWINS can help you place cyberliability coverage for your clients, reach out to your local AmWINS broker or marketing@amwins.com.

If you do not have a contact at AmWINS to help with your financial services risks, [click here for a list of brokers on our website](#).

Legal Disclaimer: Views expressed here do not constitute legal advice. The information contained herein is for general guidance of matter only and not for the purpose of providing legal advice. Discussion of insurance policy language is descriptive only. Every policy has different policy language. Coverage afforded under any insurance policy issued is subject to individual policy terms and conditions. Please refer to your policy for the actual language.

 AmWINS
Group, Inc.

AmWINS Group, Inc. is a leading wholesale distributor of specialty insurance products and services. AmWINS has expertise across a diversified mix of property, casualty and group benefits products. AmWINS also offers value-added services to support some of these products, including product development, underwriting, premium and claims administration and actuarial services. With over 1,800 employees located in 16 countries, AmWINS handles over \$5 billion in premium annually through our four divisions: Brokerage, Underwriting, Group Benefits and International.

record keeping, book keeping, administrative services and other financial services, may have the greatest exposure to this sharing of liability. See <http://www.hipaasurvivalguide.com/hipaa-regulations/160-103.php> for more information.

Procedures after a Loss. Businesses that do not have a Privacy & Security insurance policy and suffer a data breach will need to follow these guidelines:

1. Get Help

- Identify and engage a qualified attorney who will help navigate the breach notification requirements in states where potential victims reside.
- Identify and engage forensic specialists to determine what information was lost.
- If you have one, follow your breach response plan.

2. Report

- Notify the proper governmental agencies (State Attorney General, Department of Health and Human Services, Federal Trade Commission, Department of Commerce, FBI, etc.).
- Notify the potential victims and identify what information was lost and what you are doing about it.

3. Pay Up

- Pay for credit monitoring and identity rehabilitation services if necessary.
- Pay public relations firms to rehabilitate your image and bring back customers.
- Defend yourself from governmental investigations, fines, penalties and restitution funds.

4. Wait

- Hope that the records do not end up in the hands of people who will do harm to the victims.
- Hope that you have handled the breach in a way that will not result in a lawsuit.

However, businesses with a comprehensive Privacy & Security insurance policy will likely need to place one phone call, to the insurer, who will manage the rest of the process. A good Privacy & Security insurance policy (also known as Cyberliability) will include coverage of expenses for IT forensics, legal forensics, public relations, notification, credit monitoring, identity repair services, cyber extortion demands, regulatory defense and penalties, restitution funds, litigation defense and more. Insurers have already coordinated top quality vendors and law firms to handle the data breach from start to finish.

Tools to Help Businesses Understand Their Exposure. There are several valuable tools available to help understand a firm's exposure. One example is Symantec's free tool that estimates a firm's exposure to a data breach and the likely resulting expenses: <http://databreachcalculator.com.sapin.arvixe.com/>.

Symantec has also recommended that organizations implement the following best practices, whether or not they have suffered a data breach:

- 1) Assess risks by identifying and classifying confidential information.
- 2) Educate employees on information protection policies and procedures, then hold them accountable.
- 3) Deploy [data loss prevention](#) technologies that enable policy compliance and enforcement.
- 4) Proactively [encrypt](#) laptops to minimize consequences of a lost device.
- 5) Integrate information protection practices into business processes.

Conclusion. A data breach is a nearly inevitable event that requires proper preparation, planning and insurance. Some firms feel they have removed exposure through the use of encryption and firewalls. However, electronic security has been easily thwarted numerous times by employee errors, non-digital (paper) records, rogue employees, mistakes by third parties (such as record storage firms), couriers and web hosts. Data breaches caused by third parties that handle data on a company's behalf caused nearly 40% of the data breaches reported in the Ponemon Study. A company's firewall or encryption can't prevent the errors of others operating outside of the company. Negligence accounts for just over 40% of data breaches according to the study. If employees are not following preventative measures, a data breach remains a real possibility. Data losses caused by a third party handling a company's records or that result from employee error are insurable risks on many policy forms.

Having the proper pre-breach plans and safeguards in place remains critical. Purchasing the proper insurance is also an essential component. With 30+ insurance companies offering dedicated Privacy & Security insurance, premiums are competitive and affordable when compared to the liability of losing data. Many buyers are motivated by more than the potential for damages. An insurance company partner who brings a high quality breach response team and a plan to manage most aspects of a data breach is an invaluable resource to a firm facing the aftermath of a breach.

David Lewison authored this article. David is employed by AmWINS Group, Inc. and supports the Financial Services Practice.