

With the exception of Alabama, Kentucky, New Mexico and South Dakota, all states have enacted security breach laws applicable to both businesses and state agencies. (Source: National Conference of State Legislatures). It is also critical to remember that the notification laws apply according to where the victim resides. If you have a data breach involving the personally identifiable information (PII) of a resident from another state, you will need to follow the notification requirements of their home state (visit NCSL.org for state specific notification requirements). According to datalossdb, there have been over 125 million records compromised this year, compared to 27 million records compromised in 2010 and 190 million records in 2009. Given that 17% of these losses are by governmental entities, public entities need a plan in place to deal with a loss of PII, as well as a line item in their annual budget to deal with a data breach involving PII.

“Information exists in a lot of different formats in a lot of different places and is a difficult thing to control. Preventing the accidental disclosure of information is a difficult task. School districts, municipalities and other government entities are often subject to the same notification requirements and potential legal liabilities as commercial entities. They should adopt reasonable risk controls to prevent the disclosure of information and consider the purchase of insurance to pay the resulting costs when accidental disclosures cannot be prevented.”

-Nicholas Economidis, Underwriter, Beazley Group

Following is a sample of breaches involving public entities and governmental agencies.

Name ¹	Date	Type of Breach	Number of Records
U.S. Department of Veteran Affairs	5/22/2006	Stolen Computer	26,500,000
U.S. Department of Veteran Affairs	11/16/2007	Fraud	1,800,000
State of Ohio	6/15/2007	Stolen Storage Device	1,300,000
Chicago Board of Election	10/24/2006	Web	780,000
CA Public Employees Retirement System	8/22/2007	Mail	445,000
U.S. Department of Agriculture	2/16/2006	Mail	350,000
Mesa County Colorado	12/4/2010	Web	200,000
City of Chicago	9/1/2006	Stolen Laptop	38,443
City of Baytown, Texas	7/27/2009	Email	10,019
City of Savannah	9/20/2006	Web	8,800
City of Charlotte	5/26/2010	Lost Storage Device	5,220

While not all inclusive, this provides examples of large breaches as well as breaches involving cities, states and other governmental agencies. You can see that data breaches come in all shapes and sizes from a variety of public entities.

The 2010 Annual Study “U.S. Cost of a Data Breach”, which is conducted by the Ponemon Institute, shows the average cost of a data breach by a public entity is \$81 per record. By comparison, the average cost of a data breach by a business in the private sector is over \$200 per record. This average cost should be used for a “rule of thumb” for estimating potential expenses following a data breach. For example, a town with 30,000 residents and 600 employees will likely hold at least 30,600 records. In reality, they are likely holding the records of former residents and employees going back several years. If these records are not encrypted or destroyed, the town is at risk of suffering a loss due to a data breach. Since the odds of losing

To learn more about how AmWINS can help you place cyberliability insurance, 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](#).

Also, a list of public entity brokers can be found [here](#).

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. 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 2,000 employees located in 16 countries, AmWINS handles over \$5.7 billion in premium annually through our four divisions: Brokerage, Underwriting, Group Benefits and International.

(continued on next page)

100% of stored records is fairly unlikely, we'll assume for this example that the town holds 100,000 records of current and former residents and they lose 10% of the data, either by accident or hacker attack. A loss of 10,000 records at \$81 per records could cost nearly \$810,000 before litigation, damages and settlements.

Cyberliability or Security & Privacy Insurance was specifically designed to address this otherwise uninsured exposure. Consider the following types of coverage and where they fall short when it comes to covering a data breach:

Type of Coverage	Why it doesn't apply to a data breach
General Liability (GL)	GL policies cover bodily injury and property damage claims, not stolen identities. Attempts have been made to cover this exposure under advertising injury, but that window is closing. It is a real stretch to categorize a data spill as advertising.
Property	Property policies don't consider data as tangible property and does not cover identity information.
Crime or Employee Dishonesty	Crime insurance covers the theft of money, securities and property by employees. Identity information is not money or property. There is also no coverage for notification, credit monitoring or other liabilities arising from a data breach.
Public Officials or other Professional Liability	Public Officials and Professional policies respond to demands for damages. It is possible that some policies are written broadly enough to address a claim alleging an error in safeguarding information or invasion of privacy. That will only benefit you once you have been sued. Prior to being sued, you will have expended a large amount on forensics, legal costs, notification and will have likely offered credit monitoring.

Buying a Policy

What is covered by a properly constructed Cyberliability policy?

- **Network Security** – Covers your liability when hackers use your computer network to inflict damage on others.
- **Privacy** – Covers your liability when private information is disclosed.
 - **Notification Expenses** – When data is lost, you must notify all potential victims in a short period of time.
 - **Credit Monitoring** – Policies will cover up to one year of credit monitoring services for those exposed.
 - **Credit or Identity Repair Services** – Covers one year of services to repair credit or restore a victim's identity resulting from actual identity theft.
 - **Computer and legal forensic expenses**
- **Crisis Management** – Public relations consultant expenses to protect your reputation.
- **Regulatory Defense and Expenses** – Provides defense cost coverage and in some cases covers penalties where insurable.
- **Electronic Media** – Will pick up where a GL policy's advertising injury coverage stops for things like libel, slander and copyright infringement regarding your website content.
- **Cyberextortion** – Covers expenses and ransom if a hacker threatens to shut down your network or release private records.
- **First-Party Data Asset** – Covers expense to recover data you have lost due to a computer virus or hacker attack.
- **Coverage for records stored in any format and in any location** including paper records, digital records, records on laptops or other portable storage devices as well as your records stored by third parties, such as record storage firms or software application vendors.
- **Coverage for the activities of rogue employees.** You cannot control the activities of every employee. Employees often know how to access the most critical information. Most policies contain intentional acts exclusions so you need to be sure you have coverage for all innocent parties.

Procedures after a Loss

It is critical to have the proper pre-breach plans and safeguards in place, including the purchase of the proper insurance. With 30+ insurance companies offering dedicated Privacy & Security insurance, premiums are competitive and affordable when compared to the liability of losing data. Public entities that do not have a Privacy & Security insurance policy and suffer a data breach will need to consider the guidelines outlined in our earlier Client Advisory titled ["I lost my laptop. Now what?"](#)

(continued on next page)

CLIENT ADVISORY

Public Entities Are Not Immune to Cyberliability

However, entities 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. Many insurers have already coordinated top quality vendors and law firms to handle the data breach from start to finish.

“Stolen laptops have typically been the most frequent cause of a data breach; however, in the past two years it has been replaced at the top of the list by hacking events as we continue to see more targeted attacks. Given the high level of animosity that exists toward many public entities today the only real way to protect budgets and residents’ privacy is a solid data security plan backed by effective insurance.”

-Jake Kouns, Director at Markel Insurance Company and CEO of the Open Security Foundation

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. An entity’s firewall or encryption can’t prevent the errors of others operating outside of the entity. 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 an entity’s records or that result from employee error are insurable risks on many policy forms.

Premiums are typically a fraction of an uninsured loss. Further, many insureds are motivated by more than the potential for damages; they want the protection of an insurance company partner who brings a high quality breach response team and a plan to manage most aspects of a data breach. The coverage specialists at AmWINS are readily available to assist you in selecting the proper coverage for your insureds.

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

¹ DataLossDB.org