AmWINS Group, Inc.

CLIENT ADVISORY

CYBER LIABILITY INSURANCE COVERAGE FOR FINANCIAL INSTITUTIONS

A significant number of financial institutions have been victimized in recent months and years. Among those publicly acknowledging breaches were J.P. Morgan Chase, Bank of America, Citigroup, Sovereign Bank and Royal Bank of Scotland (RBS). Numerous smaller institutions have also been targeted by hackers and phishers.

RECENT BREACHES AT FINANCIAL INSTITUTIONS

Total Bank (Miami, FL)

In July 2014, the bank notified 72,500 customers that their account information was potentially exposed after an unauthorized third party gained access to the bank's computer network. Information obtained by this unauthorized third party included names, addresses, account numbers, account balances, Social Security numbers and driver's license numbers. The bank is offering 12 months free of credit monitoring services for those that were affected.

St. Mary's Bank (Manchester, NH)

A malware infestation was first detected on the computer of one of the employees of St. Mary's Bank on May 26, 2013. A computer security consultancy was called in to analyze the breach. It found that 23 workstations at the bank were hijacked by the malware. The bank notified 115,775 customers in New Hampshire about the security breach.

Belmont Savings Bank (Boston, MA)

The bank agreed to pay a fine of $7,500 related to a consumer data breach case with the Massachusetts attorney general's office. In May 2011, a bank employee left a backup tape on a desk rather than storing it. A cleaning crew disposed of the tape later that night. Names, Social Security numbers and account numbers were exposed. The tape contained the personal information of over 13,000 customers, but is believed to have been incinerated after disposal along with other sensitive materials from Belmont Savings Bank.

According to a 2013 study from cyber risk and data breach service provider NetDiligence, the average cost of a data breach is $307 per record, which includes notification costs, credit monitoring services, public relations expenses, forensics, regulatory fines and penalties, call center services, liability arising from customer lawsuits, and so on. Other studies, such as the Ponemon Institute's 2014 Annual Cost of a Data Breach Study, show that the per capita cost of a data breach for financial institutions is $206 versus an overall all industry mean of $145 per record. Many of the costs of a data breach can be transferred to an insurance policy.

However, there is little measurable data on the lost value of one's brand after a breach. An organization may suffer reputational damage that might cause a company's stock price to plummet which is a loss in shareholder value, or lose significant amounts of customers. The aftershocks following a data breach can be particularly catastrophic for a financial institution. Financial institutions are built on the trust that they will safeguard their customers' financial wellbeing in addition to confidential account information. The 2014 Ponemon study points out that one of the top two industries to have customer churn following a breach is the financial sector. The study also shows that U.S. companies have the highest lost business costs of any country, with an average of $3.3 million. Those lost business costs are calculated by "abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill."

(continued on next page)

CONTACT

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

AmWINS Group, Inc.

CLIENT ADVISORY

CYBER LIABILITY INSURANCE COVERAGE FOR FINANCIAL INSTITUTIONS

(continued from previous page)

To help combat that loss of brand value and customer churn, new cyber insurance products – mostly available in the Lloyd's of London marketplace – have started to tackle this risk directly. There are now policies that include "brand" or "reputation" damage coverage. In short, here is how this coverage would work:

- After a breach is suffered by an insured, the carrier will hire a forensic accountant to monitor the company's financial results over the course of the next few months or years (depending on policy language).
- The accountant will look for changes in revenue and/or net income during the specified time period and compare to historical and peer data.
- If there is a quantifiable drop in the insured's bottom line, the insurance policy is meant to reimburse the insured for lost net income.

This coverage is particularly intriguing for financial institutions, as they are held to a higher standard for protecting their customers' information given their role in protecting their money. In the event of a data breach, banks and other financial institutions will likely lose customers that will no longer do business with the firm because they have lost trust in the company. Imagine if a financial institution lost its largest borrower or customer as a result of a data breach. Would the company be able to survive a catastrophic event?

In the absence of – or in addition to – the participation of an insurance solution, organizations can take other steps to try to reduce their reputational exposure. Understanding what information they hold and what it means is an important first step. They should prepare for the worst case scenario as well as realistic scenarios; there should be a plan ready to roll out quickly in the event of a data breach. The organization should utilize a team with different skill sets to formulize their plans, and then speak with one voice. Organizations should consider only talking about the situation after seeking the assistance of a public relations expert. Being transparent and honest about the circumstances is also critical. These data breaches are going to happen; how organizations handle them will determine how they are viewed by their customers going forward.

As a specialty broker, we can help you place even the most challenging cyber liability risks. AmWINS brokers have access to a variety of proprietary tools and resources to assist with marketing, negotiating coverage and providing the best insurance solutions in addition to claim advocacy. Add that to our unmatched market access and superior customer service, and we are well prepared to serve the needs of retail agents and their clients.

This article was authored by Joe Catalano of AmWINS Brokerage of Illinois. Joe is a member of AmWINS' national Financial Services Practice.