



# INSURANCE IS AN IMPORTANT TOOL IN CYBER RISK MITIGATION

The time to prepare for a potential cyber attack is now, and a cyber insurance policy could be a vital piece of your risk management strategy. Here's how to make your institution more attractive to insurers and ensure you have sufficient coverage.

**BY ANNMARIE GIBLIN**

UNLIKE AN IMPENDING STORM, it is almost impossible to predict exactly when a cyber attack will occur, which is why mitigation is so crucial. The threat to institutions is real, the resulting losses can be devastating, and the time to prepare is now.

This article provides an overview of the cyber risks faced by financial institutions. While it describes in general the mitigation plans that should be enacted, it focuses more specifically on the use of cyber insurance as an important tool. In particular, it includes advice on obtaining the best policy for your institution and becoming a more attractive risk to the underwriter (hopefully, resulting in better rates and terms). It also discusses the basic terms that any good cyber liability policy will include and possible riders that should be considered.

It is important to note that the area of cyber risk mitigation is constantly evolving and so are the insurance policies. This is largely due to the ever-changing sophistication of the attacks and breaches, the security measures that are designed to help institutions, and the insurance industry's understanding of it all. Laws are constantly changing to keep up with these threats. Continuing education on cyber risk mitigation should be a priority for your risk management team and for your institution as a whole.

## Current Cyber Risks

In many ways, financial institutions have been at the forefront of cyber security and were aware of the risks well before any other industry. This is not only because of the target placed on financial institutions due to the nature of their business, but

also because the industry was one of the first to face regulations in regard to the sharing and storing of personal information. Unfortunately, despite this foresight, financial institutions have not prepared any better than other industries and, in many ways, they have suffered some of the largest losses. The threats faced by a financial institution are constant and serious.

One large problem is that not only are attacks becoming more sophisticated and frequent, but information about them is often shared too late, if shared at all.

In July 2014, the Department of Homeland Security's National Protection and Programs Directorate (NPPD) released a report, "Insurance for Cyber-Related Critical Infrastructure Loss: Key Issues,"<sup>1</sup> which was a product of round tables and workshops between October 2012 and November 2013. According to the report, the gatherings "examined the ability of insurance carriers to offer relevant cyber risk coverage at reasonable prices in return for an insured's adoption of cyber risk management controls and procedures that improve its cyber risk posture."

The report focused on first-party coverage, defined as "policies designed to transfer a company's own residual, direct costs from a cyber incident to carriers." It

# JUST AS THE TYPES OF BREACHES ARE GROWING AND CHANGING, THE TYPES OF LOSSES THAT BUSINESSES FACE ARE INCREASING AS WELL.

found that insurance carriers had limited cyber insurance offerings when it came to “coverage for critical infrastructure loss,” largely because of “a lack of actuarial data, aggregation concerns, and the unknowable nature of all potential cyber threat vectors.”

The majority of the report discussed creating a cyber incident information-sharing/data repository to fill the large information gap that exists about these incidents. The report noted that “insurance work revolves around predicting loss—specifically, the frequency of actual events, their likelihood, and their associated damages. Cyber incidents are difficult to quantify according to these measures...because there is not yet a significant history from which to draw data.”

Although steps are being taken to improve the sharing of threat information among institutions and government agencies (see previous article, “Regulators Focused on Community Banks’ Cyber Security”), currently no repository of details on past breaches exists. A repository may be very difficult to create because, as the report acknowledged, not only are cyber incidents hard to define, but “concerns about potential liability, unwillingness to apply scarce resources to information sharing, and simple apathy all might combine to diminish the urgency of corporate leaders to participate.”

Additionally, available information

about cyber attacks and breaches generally analyzes data from the past few months or the previous year, and it largely depends on the gathering of information, the reporting of cyber incidents, and the discovery of attacks and breaches—activities that are not handled consistently across the industry.<sup>2</sup>

The types of breaches that can be and are suffered by businesses and institutions are constantly changing. In the past year, phishing has become a highly publicized area of concern and can be used as an entry point to install malware on a system. Furthermore, bring-your-own-device (BYOD) policies, in which institutions allow their employees to use their own personal devices (tablets, phones, etc.) for work purposes, have become popular and are another large area of concern. These devices have direct access to an institution’s network, but often do not have the same level of security as an institution’s internal computer networks. Thus, it is hard to predict which types of known attacks and breaches will be of most concern in the future and even more difficult to predict the new types of attacks that will emerge.

## How Cyber Attacks Cost Banks

Just as the types of breaches are growing and changing, the types of losses that businesses face are increasing as well. The Ponemon Institute found that, in 2013,

the per capita cost for data breaches in the industry was \$215.<sup>3</sup> This number can increase dramatically, depending on the type of breach and the response required. Indeed, responding to a cyber incident can be very costly:

**1. Notification costs:** Currently, 47 U.S. states or territories require notification of security breaches involving personally identifiable information.<sup>4</sup> The various laws can have different definitions of personal information, as well as different requirements for notification. Costs can run very high, depending on the size of the breach and the extent of notifications required.

• In addition to state laws, the federal Gramm-Leach-Bliley Act requires institutions to ensure the security and confidentiality of customers’ personal information. It does not include specific notification laws, but the Federal Trade Commission does advise institutions to notify customers, law enforcement, and/or other businesses. This is in addition to the obligations imposed on institutions to properly dispose of any consumer information, pursuant to the OCC guidelines of the Fair Credit Reporting Act.

• Additionally, the Securities and Exchange Commission’s CF Disclosure Guidance Topic No. 2, Cybersecurity, outlines the necessary disclosures, including information to be provided, in the event of a breach. The guidance notes that the accounting for the capitalization of preventative measures costs may be addressed by the Accounting Standards Codification 350-40, Internal-Use Software. The guidance explains how cyber incidents may affect reporting to the SEC and provides direction on how to maintain compliance. It also notes that registrants must disclose conclusions on the effectiveness of disclosure controls and procedures.

**2. Forensic services costs:** Hiring professionals to determine how the breach occurred and what was taken involves

sizable costs, including the following:

- *Credit monitoring and other fraud services costs:* Providing these services to affected customers to prevent identify theft and other damages.
- *Legal fees:* Hiring an attorney or legal firm to help with notification laws, legal guidance, possible pre-litigation investigation, possible defense of regulatory proceedings, and mitigation of potential damages.
- *Public relations costs:* Hiring professionals to manage and control how the news of the breach is made public and to coordinate the response to customer and media inquiries.
- *Business interruption prevention costs:* Costs associated with hiring experts and performing other actions in response to possible service disruptions, loss of necessary information, and/or complete shutdown of necessary systems to prevent a delay or halt of business.
- *Legal costs and fines:* Beyond the payment of legal fees to defend and respond to a breach, costs could include possible civil and securities judgment awards from resulting lawsuits, settlements of civil and securities litigation, regulatory fines, and payment card insurer fines.

All of these costs can be significant. A survey of actual insurance claims related to cyber attacks and breaches reported between 2010 and 2012 revealed that the median cost for crisis services (including notification, forensics, credit monitoring, and legal guidance) was \$209,625, and the average cost was \$737,473. The median cost for legal defense was \$7,500, with the average at \$574,984. Meanwhile, the median cost for legal settlement was \$22,500, while the average was \$574,984.<sup>5</sup> In 2013, lost-business costs represented the largest financial consequence of a breach for the industry.<sup>6</sup>

### Obtaining a Cyber Insurance Policy

The practice of cyber risk mitigation is constantly evolving. There are, however, some standard best practices. Coincidentally, these best practices will also put the

institution in a better position to obtain a cyber insurance policy.

Cyber insurance is a relatively new line for many companies. For many carriers, it was a difficult product to bring to market because the risks are still not fully defined or understood. These policies are expected to continue evolving as incidents occur and claims are made. And as actual claims are filed and litigated, the law will further define and change this landscape.

The main motivation for obtaining a cyber policy is to cover losses and costs from a cyber incident. Since many institutions are already insured for other risks, a cyber policy can be used to fill in gaps that may exist in existing coverage. For example, an institution may have a policy that covers business-interruption costs. However, the definition of an incident under that policy may not include (and, if the policy has been renewed recently, most likely will not include) a cyber incident. Indeed, an increasingly commonplace exemption clause written into insurance policies is one that specifically excludes cyber incidents. As noted in the aforementioned Homeland Security cyber insurance report, “Carriers are beginning to exclude cyber risk from more traditional lines of coverage in favor of stand alone cyber security insurance lines of coverage.”

A best practice for obtaining cyber insurance is to purchase a policy that covers first- and third-party losses directly and also have your institution named as an additional insurer under third-party vendors’ cyber insurance policies. Furthermore, any contracts with third-party vendors allowing them access to internal systems or information should include clearly written indemnification provisions that cover the institution in the event of a breach caused by the third-party vendor.

It is also important to obtain a declaration sheet for the policy from the third-party vendor in order to ensure that the institution is properly covered under the policy and that the vendor has adequate insurance in the event of a breach. This is especially critical in light of the expectations placed on institutions to monitor

and wisely select third-party vendors.<sup>7</sup>

Before your institution renews or purchases a policy, there are basic mitigation actions that will make the institution a more attractive risk and help protect it from liability:

1. *Draft and continually update a written security policy:* The policy should detail your efforts to prevent cyber attacks and breaches, as well as identify areas of concern regarding possible vulnerabilities and best practices to secure points of entry. It should include industry-specific preventions, such as regularly checking ATM machines for card skimmers, and detail the plan to put safeguards into action. It should also address the types of information stored by the institution and ways to protect it. Further, it should include rules on how employees are to store and disseminate information and how they are to be regularly evaluated and updated on ways to keep current with emerging threats and responses.
2. *Educate employees about the security policy and cyber risk:* The written policy will be of no use if employees don’t know what it is or what it mandates. Employees are the front line in preventing attacks, and they must be constantly reminded of this threat and their role in protecting against it. Consider incorporating quarterly discussions or meetings with employees to discuss cyber risk and security.
3. *Draft and continually update a comprehensive Incident Response Plan:* An Incident Response Plan should lay out in sufficient detail what response the institution will take in the event of a breach. It should include key members of the institution who will be called upon and what role they will play. It should also designate a team of professionals to be notified and called upon in the event of an incident, including 1) a forensics professional (to conduct the breach/attack investigation and stop the release of information); 2) a legal professional

# CYBER RISK IS ONE OF THE MOST IMPORTANT RISK AREAS AFFECTING FINANCIAL INSTITUTIONS TODAY.

(to conduct pre-litigation activities, defend against regulatory proceedings, and advise on the resulting legal issues and notification requirements); and 3) a public relations professional (to help disseminate incident information to the public, clients, and business partners). Additionally, the plan should address the responses that must be taken both immediately and within the first few weeks of an incident, such as notification of customers and law enforcement.

#### 4. *Perform penetration testing on the system:*

Penetration testing should be done internally, as well as externally if possible. Depending on the size and resources of the institution, it should be done as often as possible, but at least once a year. Keep copies of the results for future use and to present to an insurance company to negotiate rates. The more often you conduct penetration testing and have proof of the results, the better prepared your system will be to thwart the latest types of attacks. Testing will also help expose weaknesses in your system and plug these holes.

#### 5. *Encrypt mobile devices:*

Mobile devices remain a large “soft” target for gaining access to a system. These devices, especially those provided by the institution, should be encrypted and have a wipe feature in the event they are lost or stolen. If the institution has a BYOD policy, the use of a secure connection—for example, requiring that employees access e-mail through a secure, password-protected website—may be an added level of protection.

#### 6. *Conduct a cyber breach “fire” drill:*

At least once a year, put these policies into action by simulating an attack or

breach. The fact that the event is a drill should be known only to a few key players in order to accurately evaluate the response and adherence to the Incident Response Plan. After the drill, conduct an evaluation of the response and the plan to correct any problems and/or update the plan to address concerns that were not apparent prior to the exercise.

#### Essential Provisions and Potential Riders

The needs of each institution will vary, and it is important to discuss those needs with your insurance professional to tailor a cyber insurance policy accordingly. There are, however, some essential provisions that should be included:

- Coverage for defense expenses, awards, and settlements in connection with a lawsuit.
- Coverage for notification/crisis management expenses, which can include costs for legal counsel, public relations, forensics, drafting and dissemination of notices, and credit monitoring.
- Coverage for business interruption and extra expense, which pertains to lost income and any expenses to facilitate the institution’s return to business.
- Coverage for electronic vandalism, such as erased media and electronic data corrupted in the event of a cyber incident.
- Coverage for extortion, which will cover ransoms for hackers who hold a network or data hostage.
- Coverage for fines, penalties, and defense costs in regulatory proceedings.
- Coverage for both first- and third-party losses.

Potential add-on or rider provisions that should be considered, and may be necessary depending on the terms of the policy, are as follows:

- Enhanced business-interruption coverage (in the event of a much-larger-than-anticipated event).
- Enhanced theft-of-money coverage (to close the gap on more traditional coverage).
- Hacking endorsement (to more broadly cover this risk).
- Third-party-vendor endorsement (to cover liability created by third-party vendors).
- Rogue-employee endorsement (to cover intentional acts by employees that cause harm, such as when an employee steals information).
- General negligence (to cover against accidents, such as when a laptop or briefcase is lost).
- Unencrypted-mobile-device endorsement (to protect against BYOD policies).
- Written-paper endorsement (to cover physical and document breaches, such as when someone takes information kept on paper or when the loss of important documents occurs).


Consider bundling cyber insurance with existing policies. There has been some favorable case law that indicates denial of coverage can be avoided in certain situations when insurance policies are bundled. Consider different divisions of the institution, especially if they have different corporate names, and be sure to add them to the policy or provide for them in some way. If a cyber incident originates through one of these other divisions, and that division is not specifically named in the policy, coverage could be denied.

Remember that an insurance policy is a contract—meaning that both the institution and the insurance company are entitled to the “benefit of the bargain.” If there is a provision excluding coverage or if a provision is narrowly defined, either can be used to deny coverage, giving the insurance company the benefit of the bargain. It is important to read the policy fully and make sure its definitions and provisions cover the cyber risks to the institution sufficiently.

Finally, be mindful of notice obligations in your policy (or the overall bundled policy) in the event of a breach. Late

notice is one of the most common reasons insurance companies give for denying coverage, and courts are not reluctant to uphold a denial based on late notice. In the event of a cyber incident, provide timely written notice to the insurer to make certain the policy's provisions are triggered.

### Conclusion

Cyber risk is one of the most important risk areas affecting financial institutions today. It is important to keep this area a focus of the institution's overall risk management efforts and to continually renew and update the cyber insurance policy. 

**Annmarie Giblin, Esq.**, is an attorney with the law firm Leader & Berkon LLP and is resident in the firm's New York office. She is a litigation attorney

who focuses her practice in commercial, toxic tort, and product liability litigation. She can be reached at [agiblin@leaderberkon.com](mailto:agiblin@leaderberkon.com).

This article and the information contained within is for informational purposes only. Nothing contained within is intended to be used or relied on as Legal Advice or opinion.

### Notes

1. This report can be accessed in its entirety at [http://www.dhs.gov/sites/default/files/publications/July%202014%20Insurance%20Industry%20Working%20Session\\_1.pdf](http://www.dhs.gov/sites/default/files/publications/July%202014%20Insurance%20Industry%20Working%20Session_1.pdf).
2. For example, Symantec provides monthly Internet Security Threat Reports, available at [http://www.symantec.com/security\\_response/publications/monthlythreatreport.jsp](http://www.symantec.com/security_response/publications/monthlythreatreport.jsp).
3. *2013 Cost of Data Breach Study: Global Analysis*, Ponemon Institute Research Report, May 2013, available at <http://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf>.
4. States that currently have no security breach laws are Alabama, New Mexico, and South Dakota.



See [www.ncsl.org](http://www.ncsl.org) for more information about current and pending cyber security legislation.

5. All information is from *NetDiligence 2013 Cyber Liability & Data Breach Insurance Claims: A Study of Actual Claim Payouts*, by Mark Greisiger. The entire report is available at <http://netdiligence.com/files/CyberClaimsStudy-2013.pdf>.
6. See footnote 3.
7. Third-Party Relationships, OCC Bulletin 2013-29, available at <http://occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html>.

# THE STRESS TESTING Trifecta!

Not a gamble with Credit Stress Analytics<sup>®</sup> from FIMAC Solutions<sup>™</sup>.

**Credit Stress Analytics<sup>®</sup>**  
**THREE STRESS TESTING MODELS! One Suite!**

The unlimited filtering, concentration analysis, and more that **CRE Stress Analytics<sup>®</sup>**, **Construction Stress Analytics<sup>®</sup>**, and **C&I Stress Analytics<sup>®</sup>** provide are now available in a single package.

FIMAC Solutions • [www.fimacsolutions.com](http://www.fimacsolutions.com)  
Toll Free 877.322.1880

