Cybersecurity—What You Need to Know Now

Related Professionals

Kimberly J. Schaefer

Related Services

Corporate and Business Organizations

Finance

Related Industries

Financial Institutions

AUTHORED ARTICLE | Winter 2016

Published in the Winter 2016 issue of *The Bankers' Statement*

It's all over the news and it's top of mind with bank regulators: "Cybersecurity." What happened with Target, Home Depot and Wyndham hasn't helped. The last several years have been fraught with news story after news story about those crafty hackers who find vulnerabilities in a company's system and steal private information or even redirect funds. And despite all of our technological advancements, the escalation in successful hacking attempts has no end in sight. Call them hackers, fraudsters or good old-fashioned crooks, from computer-savvy teenagers to state-sponsored groups, they are not going away. And, unfortunately, they seem at times to be two steps ahead of the latest security software and security vendors that are offering you and your financial institution protection.

What is Going on?

Cybersecurity has become banking regulators' number one priority and will be a very important hot button for current and future exams. It's obvious why this might be so—financial institutions play a particularly important role in our economy, take and hold deposits from the public at large, and, therefore, have in their possession not only customer funds but important confidential customer information. Customers come to your bank so that you can guard their financial assets; they expect full protection.

As early as 2002, the Gramm-Leach Bliley Act imposed on financial institutions a requirement to develop a comprehensive security and privacy program. This requirement has only become more focused with the FFIEC's release in June of its Cybersecurity Assessment Tool (the CAT), which can be found here http://www.ffiec.gov/cyberassessmenttool.htm. While we are not going to discuss the CAT in depth here, suffice it to say that even though the CAT has been released as an "optional" tool, it should be clear that the CAT will likely be the baseline standard for which all institutions should measure their cybersecurity protocols and protections.

The industry is on notice. Both officers and directors need to be focused on cybersecurity. So, what is cybersecurity, what are the risks involved and how can your institution mitigate those risks?

What Is Cybersecurity and What is My Role?

For financial institutions, cybersecurity refers to the means and methods used to control access to the institution's electronic data, including customers' data that is under the institution's or its vendors' control. When an institution desires to evaluate its cybersecurity protocols, it must first evaluate the risks and vulnerabilities unique to the institution and then determine what protections are in place or should be in place to mitigate those risks. Tools like the CAT are useful in providing an institution with a snapshot of where it currently stands and where it needs to place its focus.

Management's role in the cybersecurity arena is to complete this evaluation process, implement mitigation processes and continue to oversee and monitor issues. In addition, management should provide an ongoing risk assessment to the board of directors, including a report regarding any changes being made to the cybersecurity protocols or any issues that have been reported.

The board's role is to follow the enterprise risk management model-- assess the risk, utilize management and outside consultants, oversee the implementation of "best practices" to mitigate risk, monitor and enforce policies and procedures, and modify any plans as appropriate.

How Do we Assess our Cybersecurity Program?

Whether you are just developing your cybersecurity program or are performing an annual evaluation of it, your steps in assessing your cybersecurity program are the same:

First, start by evaluating your institution's risks. When looking at risks, look at every aspect of the business and do not forget the regulatory, litigation and reputational risks.

Second, assess the adequacy, or lack thereof, of your internal controls for each of these types of risks. You should perform both an internal and external assessment:

- An internal assessment is critical because it is your management team that understands your institution's risks and vulnerabilities best. You should utilize all other levels of employees as well as they can help to identify vulnerabilities and concerns first hand. You should also consider hiring third party consultants on at least an annual basis to evaluate your systems and help you identify any risks or threats that you may not have considered.
- An external assessment of your vendors must also be performed. Regulators have emphasized vendor management and due diligence for quite some time. However, it is even more critical when a vendor touches or even stores your institution's electronic data. The external assessment should include a review of the vendor's cybersecurity protocols, backup systems and insurance coverage and an evaluation of the institution's contract with the vendor to determine the allocation of risks and notice procedures in the event of a data breach.

Obviously, the FFIEC's CAT is a good place to start in assessing your cybersecurity program. There are also several other resources that you may want to consider, including:

- Financial Services Industry Information Sharing and Analysis Center (FS-ISAC)
- FFIEC IT Examination Handbook
- Cybersecurity information-sharing forums (including systems user groups)
- National Institution of Standards and Technology (NIST) cybersecurity resources

What is a Data Breach Response Plan and What Should we Do if There is a Breach?

A good cybersecurity program will include a data breach or incident response plan. This plan provides a framework for action if a data breach occurs and will ensure that key decisions are made ahead of time and do not have to be made under pressure. A good data breach response plan will:

- Identify a core team of responders who will handle the breach;
- Provide a procedure for documentation of the events leading up to and following the discovery of the breach;
- Establish a clear and immediate communication plan that includes communications to internal contacts, third parties (including law enforcement and regulators), advisors (including legal counsel and insurance carriers), customers and the media;
- Set forth key decision points that need to be made in every step of the process; and
- Include forms of notifications that can be modified to send to regulators and customers.

It is critical to coordinate with legal counsel and sometimes outside data breach consultants when developing a response plan. They will help to guide you through the process and establish the general steps you need to insure your institution responds in an appropriate manner to any potential data breach. Further, such a plan will provide a checklist of people to notify so that nothing gets missed.

In the first 24 hours after a breach, your institution will need to identify the breach and contain it, as well as ascertain that appropriate external notifications are made to law enforcement, insurance carriers, attorneys, regulators, business partners and customers. Not only do the federal banking laws have specific notification requirements, but every state where each of your customers reside may also have its own individual notice requirements It is a complicated process and fraught with significant risk for mistakes.

How do we Mitigate the Potential Liability of a Breach?

If your institution experiences a breach, your immediate concern is to contain the leak and endeavor to ensure that there is no further unauthorized disclosure or access. However, after that initial step is complete, your mind will begin to conjure up the ugly liability scenarios involving aggressive plaintiffs' lawyers and reputational damage. But, it could be even worse than you realize.

Not only may the institution experience the pain of legal action and damage to its reputation, but in both the Target and Wyndham breaches, the boards of directors were also sued for breach of fiduciary duty and waste of corporate assets. Further, Wyndham has estimated that responding to the Federal Trade

Commission's investigation alone has cost Wyndham at least $5 million. So, while the customer lawsuits are certainly something to be feared, the investigation and remediation efforts are also something to consider.

In order to mitigate these costs, your institution should consider several things. First, management should insure that it is prepared by doing the following:

- Utilize the CAT to perform an initial review of your institution's risks and vulnerabilities;
- Develop protocols and procedures to mitigate the risk of these vulnerabilities;
- Utilize experts on at least an annual basis to assist in the evaluation of your data security;
- Craft a data breach response plan;
- Obtain cyber liability insurance (discussed below); and
- Perform annual due diligence reviews of your vendors, including your vendor contracts, to insure that these vendors are also instituting policies and procedures that will mitigate data security vulnerabilities.

As has become evident in the last several years, your board of directors must be integrally involved in cybersecurity issues. As such, your directors should consider the following:

- Develop a high-level understanding of cyber-risks facing the institution;
- Make cybersecurity a regular topic of discussion with management and consider mandatory cyber-risk education;
- Periodically retain consultants to assess data-protection systems and to suggest areas for improvement;
- Designate one committee to oversee and understand cybersecurity issues, controls and procedures;
- Include a cybersecurity expert on the board or receive reports from a cybersecurity expert;
- Review the data breach response plan and insure it is updated regularly;
- Verify that directors' and officers' insurance covers data breach lawsuits; and
- Hire personnel whose sole responsibility is prevention and mitigation of cyber-attacks.

What is Cyber Liability Insurance?

Where there is a risk, there is insurance, and the development of electronic data security issues is no exception. Cyber liability insurance can be obtained for the institution and the board and will cover both third party and first party liability expenses. Right now is the time to look into it.

Coverage for third party liability expenses entails expenses such as claims expense and damages, legal defense costs and regulatory defense costs, including fines and penalties. While these expenses can be large, institutions often forget that there can be significant, and sometimes even greater, first party expenses too. First party expenses including the costs of notifying customers of the breach, crisis management and PR costs related to mitigating reputational damage, business interruption costs and costs associated with hiring a forensics company to investigate the breach. All of these costs also can be covered by cyber liability insurance.

Institutions should be aware that there may be limitations on insurance coverage. For instance, if your vendor's systems are breached, your customers still have exposure, but you may not have coverage. It is important to make sure that your cyber liability insurance covers you for both electronic data breaches and the good old-fashioned information stolen from the dumpster out back. Many cyber policies have both coverages, but not all do. Also, debit/credit card fraud is rarely covered with this type of insurance. Regulatory penalties may not, in fact, be covered. It is important to discuss specific coverages with your agent.

In this new and expanding age of cyber fraud, financial institutions must be on the offensive. For starters, use the CAT (or similar tool), develop a data breach response plan and get insured. Waiting for a data breach to occur is too late to begin thinking about these issues. Make cybersecurity a regular part of discussions with employees and the board of directors. Bring the issues to the forefront so that no one is blindsided by a cyber attack.