



Department of Commerce

Division of Financial Institutions
John R. Kasich, Governor
Andre T. Porter, Director

Week 4: Defending the Institutions

- Preparing against cybersecurity threats is not a problem that can be addressed alone. To deal with cyber risks, financial institutions must work together, work with regulators, collaborate, and share information. This will enable the sharing of best practices and techniques that are meant to help financial institutions focus resources on the most significant areas of concern.
- Addressing cybersecurity can no longer be managed as a compliance activity, where you simply ask your staff if they are following “best practices” on a check list.
- Cybersecurity must be managed as a risk management or security issue that requires an understanding of the primary cyber risks that face your institution and how those risks can be mitigated.

Management must understand what they are protecting prior to placing safeguards in place. For this reason a comprehensive risk assessment is imperative to ensure systems and processes are identified and classified based upon sensitivity. Based upon these, safeguards must be established and tested to ensure their functionality. The risk assessment is a dynamic document that changes as new technology is introduced and as risk changes. The IT Risk Assessment Process is found in the FFIEC Information Security Handbook and can be viewed here.

Week 3: Targeting Financial Institutions

- Cybersecurity is a societal issue facing all industries all across the nation, including your business customers.
- The frequency and sophistication of cyber-attacks directed at financial institutions are growing, and there is no expectation that attacks will decline. Criminals have always targeted and are increasingly targeting the banking industry. These cyber-attacks are being exacerbated by rapidly evolving and a growing reliance on digital technology, as well as increasing sector interconnectedness.
- Ensuring that financial institutions’ defenses, as well as that of their service providers, are able to protect our industry against cyber-attacks. It is important that you assess and manage the risks of your service providers. This includes ensuring that your service providers have adequate controls and processes in place to protect the institution and your customers.

The board and management can outsource functionality of many items to their vendors, but cannot outsource the responsibility and risk. Management must ensure that vendors, including technology service providers, are held to standards that protect and ensure that personally identifiable information (PII) is safeguarded at all times and the institution is notified of any breaches or potential breaches in a timely manner.

In addition, it is important that retail and commercial customers of financial institutions are also made aware of threats that may exist if they don't have adequate controls within their networks. Malicious software can exist on customers' networks that can monitor and exploit their online banking access. Financial institutions should risk rank their customers and ensure that customers are made aware of the risks with online banking if adequate controls are not established.

Week 2: Management's Role

- This threat requires a shift in thinking on the part of community bank CEOs that cybersecurity is not a backroom or IT issue, but a major issue for the board room, senior executives, and the CEO.
- CEOs and senior executives *must* play an active role in the management of cybersecurity risks. This will require that both you and I learn more about the threats facing our industry and how to manage these risks.
- Executive level knowledge of managing cyber risk is not difficult, but it is a different focus than the usual financial analysis we have. As a CEO, it is vital that you are aware of the threats of potential cyber-attacks, understand their risks, and work within your institutions, as well as with your service providers and your peers, to ensure security and resilience of your institution in the face of increasingly sophisticated cyber threats.

A financial institution is only as strong as its weakest link. Historically the weakest link has been the human link. A whole network can be compromised by a single user accessing or downloading information through a malicious website. It is imperative that management emphasize that their staff be cognizant of the cybercrime threats and can alert senior management to any suspicious activity. Ongoing security training is critical to combat cybercrime.

Information on the Conference of State Bank Supervisors (CSBS) Executive Leadership of Cybersecurity initiative is available here.

<http://www.csbs.org/cybersecurity/Pages/default.aspx>

May 7, 2014 – FFIEC Webinar: Executive Leadership of Cybersecurity: What Today's CEOs Need to Know About the Threats They Don't See.

To view the video:

<http://www.youtube.com/watch?v=t1ZgWKjynXI&feature=youtu.be>

To view the slides:

https://www.ffiec.gov/press/PDF/CCIWG_Cybersecurity_Draft18forIndustry_May7webinar.pdf

Week 1: Introduction to Cybersecurity

- Cyber-attacks seek to exploit vulnerabilities to steal money, prevent financial organizations from offering services, inflict reputational harm, and undermine confidence in the financial system.
- Recent cybersecurity breaches at retailers and sophisticated DDoS (distributed Denial of Services) attacks demonstrate that the impact to institutions and their customers goes well-beyond technology issues to include real financial and reputational implications.
- As part of an initiative to raise the awareness of financial institutions and their critical third-party service providers with respect to cybersecurity risks, the FFIEC launched a web page on cybersecurity recently that serves as a central repository for current and future FFIEC-related materials on cybersecurity. <http://www.ffiec.gov/cybersecurity.htm>. Additionally, the FFIEC recently released joint statements on two specific types of cyber-attacks, Distributed Denial of Service (DDoS) attacks and cyber-attacks on small to medium-sized institutions that result in large dollar value ATM cash-outs. You can expect to see more issuances out of the FFIEC in the future.

Cybersecurity: Part 1 — Demystifying Cyberthreats is an article from the Federal Reserve's Community Banking Connections publication describing cyber threats and cyber related risks and exposures available at the following link:

<http://www.communitybankingconnections.org/articles/2014/Q1/cybersecurity.cfm>

A supervisory bulletin was released in February 2013 providing guidance to financial institutions on "Standards for Risk Management of Corporate Account Takeovers." www.CATOBestPractices1.com The guidance refers to 19 recommended processes and controls which expand on a three part risk management framework of: 1) Protect; 2) Detect; and 3) Respond. Additionally, Best Practices for Reducing that Risks of Corporate Account Takeovers, was developed to help financial institutions establish specific practices to implement the recommended processes and controls. The Best Practice document is a valuable resource to effectively reduce risk and can be found at www.CATOBestPractices2.