SBS institute
700 S. Washington Ave. Ste. 200
Madison, SD 57042

FDIC – A Framework for Cybersecurity

Written by: Jon Waldman – Partner, CISA, CRISC - Secure Banking Solutions, LLC

A Changing Landscape of Regulation

Over the last twelve months, there have been numerous significant changes to financial institution Information Technology regulation. The FFIEC has been particularly busy, releasing topical guidance documents (Destructive Malware, Cyber Attacks Compromising Credentials, Extortion), making wholesale changes to the way it expects IT Operations to be managed via an update to the IT Management Handbook, and – of course – the big ticket item: the FFIEC Cybersecurity Assessment Tool.

Most recently, the FDIC published an article titled "A Framework for Cybersecurity" in the Winter 2015 edition of its quarterly magazine, Supervisory Insights. In this article, the FDIC highlights the fundamental basics for building protections against cyber threats into a financial institution's Information Security Program (ISP) and culture.

The Evolving Threat Landscape

As financial institution's reliance on technology has increased, so have the various types of cyber-attacks they face on a regular basis. The FDIC mentions three specific categories of attack: Malware, Distributed Denial of Services Attacks (DDoS), and Compound Attacks. Malware is a threat that you're likely already familiar with, but ransomware in particular is a very real and growing threat to businesses of all types, including financial institutions. Compound attacks tend to use DDoS attacks as a distraction technique while simultaneously attacking the institution from another vector – commonly via malware – in order to gain remote access to your network while your attention is elsewhere.

A Critical Infrastructure Perspective

The FDIC mentions Executive Order 13636 – Improving Critical Infrastructure Cybersecurity – and the subsequent NIST Framework for Improving Critical Infrastructure Cybersecurity as a strong basis for which financial institutions should look to enhance their Information Security Programs with cybersecurity processes and controls. The NIST guidance is broken into five (5) major areas: Identify, Protect, Detect, Response, and Recover.

Additionally, the FDIC mentions that a financial institution must design a cyber risk control structure that is based around four (4) components: Corporate Governance, Threat Intelligence, Security Awareness Training, and Patch Management.

Corporate Governance of Cybersecurity

As with most other recent iterations of updated guidance or documentation relating to cybersecurity, the FDIC once again mentions the importance of the top-level of our financial institutions paying more attention to and understanding cybersecurity. The Board of Directors and senior management must begin to understand and manage cyber-risks from the top of the organization and prioritizing cybersecurity in the institution's culture, because expecting it to happen from the bottom-up is not an effective strategy for managing cybersecurity.

Threat Intelligence

As with Corporate Governance of Cybersecurity, Threat Intelligence and Collaboration has been a major hot topic with regulators over the past eighteen months. The FDIC Framework for Cybersecurity emphasizes that keeping abreast of current threats affecting financial institutions is not only very important, but expected. Each institution should have a plan or program in place for gathering, analyzing, understanding, and sharing information regarding current threats and vulnerabilities in order to arrive at what the FFIEC refers to as "actionable intelligence."

The two most common ways to share and collaborate threat intelligence between financial institutions involve the FS-ISAC (Financial Services Information Sharing and Analysis Center) and the US-CERT (US Computer Emergency Readiness Team). FS-ISAC offers a free alerting system, called the CNOP (Critical Notification Only Participant) as well as a Basic membership ($250/year), for institutions under $1 billion in assets. Regulators do not consider the CNOP to meet regulatory requirements, however. The US-CERT subscription is free of charge.

Security Awareness Training

Maturing an organization's ability to protect its customer information via people is a challenge for all financial institutions, as well as one of the most important aspects of an ISP. The best technology in the world can keep the "bad guys" out, but if one employee clicks a link in an email that contains malware, all of that great technology is circumvented and rendered moot.

The FDIC highlights the need for role-specific cybersecurity awareness training and education for employees; specifically those employees that have access to confidential customer information or are involved with IT Operations. As mentioned earlier in the Corporate Governance section, the Board of Directors and all senior management must participate in security awareness training in order to ensure an effective cybersecurity awareness program.

Patch Management Programs

As the number and frequency of vulnerabilities increase each day, the importance of a strong patch management program becomes much more evident. Whether your institution is migrating away from products no longer supported by vendors or making sure the hardware, software, and applications you currently utilize are up-to-date, all institutions must implement a formal, documented, and repeatable process for identifying, testing, and implementing patches and fixes for known vulnerabilities. Statistics tell us that the vast majority of breaches (around 97%) can be prevented from simple patch management.

In order to ensure the patch management program is effective, the Board and senior management should require regular standard reporting (using metrics) regarding the patch management program. Independent audits and internal reviews should also cover the implementation and effectiveness of the institution's patch management program. The financial industry is also moving "continuous patch management," as 12-18 months is typically far too long a wait to ensure the patch management program is effective and protecting the institution and its customer data.

Regulatory Response and Resources

The FDIC also includes in this Framework for Cybersecurity a number of additional cybersecurity-related resources, including the “Cyber Challenge” exercise and related Cybersecurity Awareness videos, the Cybersecurity Critical Infrastructure Working Group, the FFIEC Cybersecurity Assessment Tool, the updated FFIEC IT Management Handbook, and additional cybersecurity-related documentation.

Conclusions

Despite not mentioning the FFIEC Cybersecurity Assessment Tool, which was released in June 2015, the FDIC highlights four (4) major foundational pieces to be sure that your financial institution is addressing in your Information Security Program. Corporate Governance, Threat Intelligence, Security Awareness, and Patch Management in-and-of-themselves do not comprise the entirety of anyone’s Cybersecurity Program or ISP. There are numerous other regulatory-based documents, including the FFIEC IT Management Handbook and the FFIEC Cybersecurity Assessment Tool, that provide a much more comprehensive approach to including cybersecurity into your ISP. However, these four (4) areas are very vital to cybersecurity, and are most certainly areas that you should be addressing in your ISP before your next regulatory examination or IT Audit.

What can SBS do to help?

Secure Banking Solutions has a team of auditors and consultants that can assist you in developing sound Information Security Program practices, such as Corporate Governance, security awareness training programs, patch management programs, and other risk mitigation strategies, as well as testing to ensure these practices are in place and working the way they should.

Additionally, the SBS Institute, the educational branch of Secure Banking Solutions, has developed eleven (11) financial institution-specific, role-based Cybersecurity Certification Programs. These certifications encompass numerous topics, including how to build and manage an ISP, which will help you manage cybersecurity, comply with regulation, and protect your institution from attacks. Over 600 students in over 30 states have already completed SBS Institute certification programs, and the number continues to grow by the day. The SBS Institute’s Cybersecurity Certification Programs are endorsed by 31 banking associations, as well as by the Graduate School of Banking.

Contact SBS by calling 605-923-8722 to speak with one of our Help Desk representatives about our services. If you have any additional questions, comments, or concerns, please let us know; we are always happy to help. For more information, please visit SBS at: https://www.protectmybank.com/