AuditOne LLC

Risk-Managed Internal Audit and Credit Review Expertise

NEWS

A Guide to Incorporating Cybersecurity into Your Bank's Information Security Program

AuditOne, LLC September 16, 2016

By Kevin Tsuei, CISA, CISSP, AuditOne, LLC

A recent FIS 2016 Risk Practices Survey finds that 77% of bank executives and board members cited cybersecurity as their top concern. In accordance with this, various interagency guidance items have been released since last summer, including the Cybersecurity Assessment Tool (CAT), revision of the FFIEC IT handbooks, and other regulatory communications. In general, we have observed that financial institution managers have been trying to not only complete the Assessment but also to implement a wide range of action plans. While regulators have stated that the CAT will not be used as part of their examination procedures, they do expect institutions to go through the exercise of assessing their cybersecurity risks. This article aims to provide institutions with questions that are often asked by our clients:

What are regulators currently looking for as evidence of preparedness for cybersecurity risks?

As with all risk management processes, it always starts with a risk assessment; as such, management is expected to update its IT/IS risk assessment based on the current threat landscape, including ransomware, a current hot topic. In addition, ensure all critical systems are covered, such as SWIFT and FedLine which have been in the news due to the Bangladesh Central Bank heist. While regulators do not expect community banks to have a separate Cybersecurity Policy, they do expect banks to incorporate cybersecurity elements into the Information Security Program. We will cover some of the key elements below.

A few of our clients have created a separate Cybersecurity Committee, in addition to the IT Steering Committee. While we do not discourage this practice, most community banks simply do not possess the resources to do this. A separate committee would require a separate charter that details membership, responsibility, authority, and meeting frequency. We do, however, recommend ensuring that the IT Steering Committee goes over cybersecurity topics such as highly visible cyber-events or regulatory alerts. In addition, if the institution has performed the voluntary FFIEC CAT,

the results should be provided and discussed (e.g., any control weaknesses, plans to mitigate those weaknesses).

We also suggest that IT/IS training should incorporate cybersecurity topics. Many resources are available, including FFIEC's own cybersecurity webpage: https://www.ffiec.gov/cybersecurity.htm. Having staff attuned to these risks can be a valuable first line of defense. One of our clients recently told us that they had found that one of the keys in getting the message across is to demonstrate how cybersecurity events can affect employees' personal lives.

Another recommendation is to review the bank's insurance for clauses covering employee fidelity, IT equipment and facilities, media reconstruction, extra expenses (including backup site expenses), E-banking activities, business interruption, valuable papers and records, errors and omissions, items in transit, and other possible risks.

If the bank relies heavily on its IT service provider, ensure the Information Security Officer (ISO) understands the pertinent cybersecurity risks (e.g., not being able to perform the CAT). In addition, ensure that the ISO has the appropriate authority to carry out responsibilities and that there are no conflicts of interest in his or her ability to make decisions in line with the bank's risk appetite. Further, management should review the composition of the Incident Response team. Generally, it should include representation from senior executives, legal, public relations, information technology, and individuals responsible for liquidity and reputation risk, vendor management, fraud detection, and customer inquiries or complaints.

How do I manage my vendor and technology service provider risk as it relates to cybersecurity?

We recommend ensuring that the incident response plan testing using simulated security incidents/scenarios (such as ransomware) is conducted periodically as part of ongoing risk assessment and training for Incident Response Team members. Testing should incorporate third-party service providers for their cyber-resiliency. This allows management to test the Incident Response Plan and ensure that it corresponds with applicable disaster recovery plans. Regulators suggest that management have disaster recovery (DR) procedures to allow up to 72 hours without the core processing system. They have noted that most core processors have a service level agreement (SLA) of 72 hours' downtime.

To understand your vendors' cybersecurity threat intelligence and resilience (applicable to core processing and IT), we recommend that management verify for all key vendors the cybersecurity controls listed in this article (i.e., incident response testing, cybersecurity policies, threat intelligence and collaboration program, etc.).

What exactly is a Threat Intelligence and Collaboration Program, and how do I implement one?

Threat Intelligence and Collaboration Programs have been mentioned in several interagency guidance statements published in the last year or so. Such programs are a relatively new control for community banks and generally have four main components: threat intelligence sources, who performs the monitoring and analysis, what is the response/mitigation plan, and information sharing. There are various sources for gathering threat intelligence. For example, external threat intelligence might include software vulnerability alerts from US-CERT and FS-ISAC red alerts. Internal threat intelligence might include information gathering from security monitoring, vulnerability assessment, and anomalies recognized once a baseline activity is established.

We have built a sample table below to demonstrate what a Threat Intelligence and Collaboration Program might look like for a community bank. Although the program might be more extensive depending on the size and complexity of the institution.

Sources	**Monitor and analysis performed by**	**Response/Mitigation Plan**	**Information Sharing**
US-CERT, FS-ISAC, FDIC FIL (FFIEC) alerts	IT personnel	Windows vulnerabilities: Contact patch management team for remediation Third party software vulnerabilities: Patch performed by IT personnel Other vulnerabilities: Contact security team for remediation	Quarterly IT/IS/Cybersecurity meeting
Quarterly Vulnerability Assessment	Management and IT personnel	Contact patch management and security team for remediation plan	Quarterly IT/IS/Cybersecurity meeting
Incident of suspected and actual breach	Management and IT personnel	Please refer to incident response plan	Please refer to incident response plan

Management can further customize their own program to include other actionable tasks to mitigate threats such as bank-wide alerts and training. We always recommend documenting these actionable items for both regulators and the Board of Directors to review.

We hope that this article is helpful to you in responding to rising regulatory expectations in this area. It will take time with continuous training, with regular communication and with experience gained from a range of security breach headlines for a cybersecurity culture to be well engrained.

Published in Western Independent Bankers Association's Technology & Security Digest, Issue 30 – September 2016.

AuditOne has been audited for compliance with the QAR requirements of the Institute for Internal Auditors (IIA).

AuditOne, LLC | LinkedIn

Address:
6131 Orangethorpe Avenue, Suite 470
Buena Park, CA 90620

Phone: 562.802.3581