Western Independent Bankers

WIB Publication

Western Independent Bankers

Technology & Security Digest

Issue #27 - September 2015

For Smaller Banks, Information Security is Paramount

By Bonnie Dallum, Moss Adams LLP

Information security breaches have become a new favorite headline for media outlets. We've all heard about attacks against major banks, such as JPMorgan Chase, but what about smaller banks? With limited IT resources compared with the Fortune 500 companies, they still store and process sensitive information that may be targeted by hackers. Though the significance of information security may not be as apparent to a smaller organization, in reality, it's just as important.

Why Is Information Security Important?

Compliance with the Gramm-Leach-Bliley Act

Smaller banks often have limited resources, and they may not be doing enough to safeguard their customers' sensitive information, which is – in the first place – a violation of the Gramm-Leach-Bliley Act.

Bank customers want the convenience of technology and telecommunications, with transactions just a click away and the assurance that their information is safe from unauthorized access. Whether your bank is the largest in the nation or the smallest, those demands ought to put cybersecurity and mitigating risk at the very top of your priority list.

Cybersecurity is one of the most important challenges facing banks today, with the threat of unauthorized access, disruption or even outright theft of information increasingly top of mind. How should smaller banks make decisions about safeguarding their customers' sensitive information with limited resources? Sure, cybersecurity can be costly, and banks need to weigh the costs with the benefits of added cybersecurity resources, but remember that while the cost of coverage can be expensive, the cost associated with a breach could be catastrophic.

Small Banks Are Easy Targets

Hackers know smaller banks have limited resources, making them favorite targets. As cyberthreats evolve rapidly and become more sophisticated, smaller banks are often hard-pressed to keep up with the latest developments, according to a 2014 report by the New York Department of Financial Services. While larger banks are more likely to spend on expensive in-house systems for protection, smaller banks may lack the resources or even awareness to implement strong cybersecurity. This leaves smaller banks more vulnerable, and because smaller banks have more to lose, cybercrime could have a debilitating effect on their business.

Assess Your Bank's Security

For starters, smaller banks should look into a layered approach of securing their environment and review the Federal Financial Institution Examination Council's (FFIEC) cybersecurity assessment tool, released this July, to see how they stand.

According to the National Institute of Standards and Technology, cybersecurity is defined as "the process of protecting information by preventing, detecting and responding to attacks." According to the FFIEC, which seeks to increase awareness of these risks for banks and their third-party service providers, the management of internal and external threats and vulnerabilities are the two issues that institutions should look at as they seek to protect information and the supporting infrastructures from technology-based attacks.

With the release of the FFIEC cybersecurity assessment tool, all banks now face expanded IT security and controls scrutiny by regulators and auditors. According to the FFIEC, some key examination areas include layered antimalware strategies, such as anomaly detection, system behavior monitoring and employee security awareness training. Management of third-party service providers also is high on the list for increased scrutiny. One of the best ways to combat the risk associated with cybersecurity is to have and follow a plan that includes proper monitoring, risk assessment, resource allocation and diligence. A good starting point is to instill a heightened awareness in all employees that the threat by fraudsters is very real and constant.

The FFIEC tool consists of two parts: your inherent risk profile and your cybersecurity maturity. The inherent risk profile section identifies the institution's inherent risk before controls are implemented. The cybersecurity maturity section includes domains, assessment factors, components and individual declarative statements across five maturity domains to identify the specific controls and practices in place. Note that while this assessment helps management determine the institution's maturity level in each domain, it isn't designed to identify an overall cybersecurity maturity level.

To complete the assessment, management first assesses the institution's inherent risk profile based on five categories:

1. Technologies and connection types
2. Delivery channels
3. Online or mobile products and technology services
4. Organizational characteristics
5. External threats

Management then evaluates the institution's cybersecurity maturity level in each of five domains:

1. Cyber-risk management and oversight
2. Threat intelligence and collaboration
3. Cybersecurity controls
4. External dependency management
5. Cyber incident management and resilience

Step Forward with Confidence

Though establishing a cybersecurity program and keeping it up to date on current threats may seem overwhelming, there are tools, resources, and cybersecurity consultants that can guide you along the way. It's an ongoing and sometimes challenging process, but in the end, it'll pay off in peace of mind – both for you and your customers.

Back to September 2015 Technology & Security Digest

Bonnie Dallum is a director with the IT Auditing & Consulting Practice at Moss Adams (www.mossadams.com). She can be reached at 415-677-8303 or bonnie.dallum@mossadams.com.