APRIL 12, 2016

INFORMATION TECHNOLOGY UPDATE

2016 Anticipated Regulatory "Hot Topics"

As 2016 is well upon us, it is no surprise to see that regulators are placing more and more emphasis on the security of financial information. During the first quarter of 2016, Snodgrass has observed the following regulatory "trends," and they appear to be new areas of focus for financial institution information technology examinations.

Cybersecurity Assessment Tool Review

A primary focus of regulators in 2016 will be on the newly created Cybersecurity Assessment Tool (CAT). While regulators generally agree that this exercise is not a "requirement" for financial institutions at this time, the tool itself contains over 400 questions which examiners will be required to complete and document as part of their examinations. Financial institution management is encouraged to complete this exercise prior to their IT examination to lessen the on-site time of the examiners and provide them with information required to complete their examination. The first step in CAT is to assess the institution's inherent risk profile in each of the following four areas:

1. Technologies and Connection Types
2. Delivery Channels
3. Organizational Characteristics
4. External Threats

In order to assess the institution's risk mitigation, questions are answered in the following "domains" of security:

1. Cyber Risk Management and Oversight
2. Threat Intelligence and Collaboration
3. Cyber Security Controls
4. External Dependency Management
5. Cyber Incident Management and Resilience

Answering questions in the above five domains helps an institution "map" its inherence risk profile. According to recent Snodgrass-attended seminars regarding CAT, regulators have agreed that the focus for the first few years of their exams will be to ensure that each institution meets the "baseline" security levels for each respective area of security covered within CAT. Over time, both institutions and regulators should shift their focus to improving an institution's security posture by adding controls in each domain to gain a higher security posture above the baseline standards.

FFIEC Revised Management IT Booklet

The FFIEC recently announced a new version of the Management Booklet within its IT Handbook that is used as the standard for financial institution Information Technology Audits. Content was added and expanded upon from previous versions in the area of IT governance. The change in the Handbook will increase scrutiny over the structure and functioning of the Technology Committee, Audit Committee, and Board of Directors with respect to their involvement in the area of Information Technology. Documentation supporting IT governance should be enhanced in anticipation.

This update is intended to provide timely, accurate, and authoritative information on the subject matter herein. Due to the general nature of this update, the information contained herein should not be acted upon without professional advice related to your specific situation.

Removable Media Controls

While this topic is certainly not new, and Snodgrass has been inquiring about controls for removable media (CD-ROM, USB “thumb” drives, external hard drives, etc.) for some time now, 2016 has brought an apparent focus by regulators for controls in this area. We are beginning to see strong recommendations or requirements by regulators for the following controls of removable media:

1. Blocking/Limiting Use of Removable Media: Following the principle of least privilege, the majority of financial institution employees would not require the use of removable media. Controls built into the Windows server environment as well as commercialized non-Windows- based tools offer the ability to block or severely limit the use of these devices.

2. Encryption: As is the trend with most mobile security devices (including tablets, cell phones, and backup media), the encryption of the data on these devices is imperative to ensure that a lost or stolen device does not lead to a customer information breach. Therefore, regulators are now beginning to require encryption on removable media as well as tablets, cell phones, and other portable devices. For years, regulators have been recommending laptop hard drive encryption. The concept of encryption of data “at-rest” is now being expanded to include other types of portable devices as well as removable media.

Questions?

If you have any questions regarding this document or the resources listed below, please feel free to contact Jeremy Burris, Rob Haller, or Chris Kreutzer at (724) 934-0344 or (800) 580-7738, or email jburris@srsnodgrass.com, rhaller@srsnodgrass.com, or ckreutzer@srsnodgrass.com.

This update is intended to provide timely, accurate, and authoritative information on the subject matter herein. Due to the general nature of this update, the information contained herein should not be acted upon without professional advice related to your specific situation.