SNODGRASS
Certified Public Accountants and Consultants

"Your Key to a Wealth of Information"

VOL. 4 | NOVEMBER 18, 2014

INFORMATION TECHNOLOGY UPDATE

Social Media and Cloud Computing

Social media and cloud computing arrangements are "hot-topics" as these two areas gain momentum in the industry. While both areas have great benefit to financial institutions, they also pose new, previously unconsidered risks to the industry. This quarter's IT Update will focus on these new risks and related requirements, providing helpful hints that should be included in your institution's policies and procedures to ensure security best practices are in place and regulatory concerns are addressed.

Social Media

Whether your institution uses social media websites for marketing purposes or not, a social media policy is both a best practice and a soon-to-be regulatory requirement. When drafting your social media policy, we suggest you consider the following topics:

- **Social Media Risk Assessment:** The starting point for a good policy is to identify the risks for your institution, determine how those risks are currently addressed, and identify any gaps that may exist. Developing a social media risk assessment is a great way to both accomplish this objective and build a framework to ensure your policy stays current as this area continues to evolve. A social media risk assessment should address the identification, measurement, monitoring, and control of risks related to social media. The size and complexity of the risk assessment will evolve over time, commensurate with the breadth of the institution's involvement in this medium.

- **Acceptable and Unacceptable Employee Usage:** Even if your institution does not use social media for marketing, the vast majority of your employees are users. Having a policy to guide them in their use of social media, particularly as it relates to the company and its customers, is critical. The policy should inform employees that posting customer-related information online is a breach of the company's privacy policy. It should stress not divulging even the most minor information online that could be construed as "insider" information. An example of this is an employee posting on Facebook that he just closed a $3 million loan with XYZ Corporation that took several months of work. As innocent as this may seem, taking a step back you can quickly see the potential ramifications. The policy should also describe acceptable uses of social media for business purposes, whether employees are allowed to visit personally owned social media websites during business hours, who at the institution is allowed to "post" information on behalf of the institution, and other acceptable and unacceptable uses of social media websites.

- **Right to Discipline Employees if They Violate the Policy:** While your employees may note that they have "freedom of speech" to post anything they want to online, it is also the institution's right to take corrective action should social media posts by an employee become a problem. These problems could include speaking negatively about the institution, posting customer information as noted above, or any number of other posts that could negatively impact

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.

your institution. The policy should clearly state that disciplinary measures can and will be taken, up to and including termination of employment, for policy violations. Seeking legal counsel's advice in this regard is prudent based on recent rulings regarding disciplinary action taken against employees for speaking out via posts about work conditions.

- **Training:** As social media continues to evolve, training and review of the social media policy with employees should be conducted regularly and the policy should be re-assessed at least annually.

For more information from a regulatory perspective, the FFIEC *Guidance on Risk Management Programs* provides additional guidance.

Cloud Computing

While cloud computing has its obvious benefits of scalability, lessened internal risk of data loss, and cost savings, these outsourced arrangements present extra risk. In general, the establishment of a cloud vendor contract and cloud vendor review is critical to reducing the amount of risk of off-site data storage to an acceptable level, and should include the following:

- The institution should assess the risk of the data to be stored in the cloud with this vendor, whether customer-related information is included, and the sensitivity of such data.

- The institution should assess the methods of transferring data to and from the storage location and ensure that appropriate security over this transfer of data exists.

- Any cloud computing arrangements should be included within the institution's overall risk assessment to ensure that the risks of using these vendors are reassessed annually.

- Contracts should include information about the security of the data being stored, as well as clearly defined responsibilities, liabilities, and breach notification clauses.

- Contracts should clearly state where the data will be stored, as well as backup and recovery-related information. Special consideration should be given to any data outside of the United States due to numerous legal and governing jurisdiction issues.

- If applicable, the contract should detail the data retention standards that will be followed, detail data ownership, provide a "right to audit" clause or ensure that auditing reports by third-party vendors are available yearly, and should not contain abnormal termination clauses.

Questions?

If you wish to discuss any of the above items, please contact Jeremy Burris or Rob Haller at (724) 934-0344, or email at jburris@srsnodgrass.com or rhaller@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.