SNODGRASS
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

"Your Key to a Wealth of Information"

VOL. 2 | APRIL 23, 2014

INFORMATION TECHNOLOGY UPDATE

Vendor Management

Over the holidays, a little company got itself into a little trouble. All right, it wasn't a little company, it was Target; and it wasn't a little trouble, it was a lot of trouble. Investigations have shown that the massive breach of customer credit card and PIN numbers at Target stemmed from undetected access that its heating and air-conditioning company had to the Target network. Target spokespeople noted that the network was supposed to be completely segregated from the network that stored customer credit card information, but this logical security control had apparently never been tested and led to a huge data breach.

With all of this attention on inadequate vendor management practices by Target, regulators have now turned their attention to this topic as it relates to financial institutions to ensure a similar breach does not occur within the financial world. A majority of the regulator vendor management comments have focused on security of customer information housed and/or accessed by vendors. Specifically:

- **Addition of *every* vendor to the risk assessment matrix** – Whether adding to an existing risk assessment or creating a specific vendor risk assessment, regulators are asking that every vendor be ranked according to the vendor's potential for reaching, seeing, or housing customer information. This process ensures that management of financial institutions gives serious thought to which vendors may or may not be able to access sensitive information. As with all risk assessments, controls listed to mitigate risk should be tested at least annually. In Target's case, this would have potentially allowed for the detection of the integrated networks with the heating and air-conditioning company and may have allowed for a better mitigation of risk had its control (the belief that the networks were segregated) been tested.

- **Review of contracts and addendums** – This should include a full review of all current contracts to ensure privacy, security, and safeguarding of customer information for vendors that potentially have access to it. While multiple-year contracts may not need to be reviewed after their initial signing, yearly addendums should be reviewed to ensure they are in line with the original contractual language in the areas noted above. Best practice is to review every contract in light of new requirements and identify any weaknesses that may need an addendum to cure. Track the review date to ensure that all potential items through that date have been identified.

- **Documented annual reviews of vendors** – Vendors that have access to (or that store) customer information should be reviewed at least annually according to the financial institution's vendor management procedures. Typical tasks associated with these reviews include a reassessment of the vendor's risk based on current access to sensitive information, vendor financial reviews, a right to audit (or review of the current SSAE 16 SOC 1 report), ownership of data, a review for adherence to any Service Level Agreements (SLAs), a confidentiality review, and reference checks (for new vendors prior to signing a contract).

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.

File and Folder Permissions

Since IT security is one of the primary risks in banking today, financial institutions should reevaluate file and folder permissions on Windows networks. Some early observations and best practice suggestions follow.

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.

Observation	Recommendation/Background
"Full" or "all" permissions are granted when not required.	**Background:** Full permission grants an extreme amount of access to the user. In addition to being able to delete files entirely, full access also gives users the ability to take ownership of files, modify attributes of the file, assign other users the rights to files that may not require such access, and other excessive permissions that can lead to accidental data corruption or fraud. **Best Practice:** "Full" permissions should be removed and replaced with the appropriate "Read," "Write," or "Execute" permissions, with thought given to which permissions each individual or group actually requires. Keep in mind, users should rarely be given access to modify or delete files within the backup location.
One user is granted access to another user's private share (often by reasoning that the user needs a backup staff member to be able to access the user's files in a pinch).	**Background:** This folder is intended as the user's private share. Assigning permissions to another user defeats that purpose and could allow the other user access to data to which that user may not be entitled. **Best Practice:** Assign permission to these private directories to a security group (such as the network administrators group or trusted financial institution officers). In a pinch, these trusted groups can pull needed files when the owner is not available.
Windows access permissions are not being periodically reviewed.	**Background:** While periodically reviewing Windows users and groups is important to ensure that only valid users have access and that group assignments are consistent with job responsibilities, access permissions also need to be periodically reviewed to ensure access remains commensurate with job responsibilities. **Best Practice:** Windows access permission should be reviewed at least annually, and access should be restricted to only necessary functions based upon users' job responsibilities and sound segregation-of-duties principles.
The built-in "everyone" permission is assigned permissions.	**Background:** While it is true that unauthenticated users cannot use the "everyone" permission if the built-in guest account is disabled, research has shown that other "guest" accounts may allow unauthenticated users access to files and folders. **Best Practice:** File and folder permissions should be assigned on an as-needed—and on a most restricted—basis. The "everyone" permission should (at a minimum) be replaced with the domain users group to ensure that only authenticated users have access to files. Generally, all domain users do not require access to files, and assigning access to the users and groups that do require access provides a more restrictive environment.

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.