

Solutions

Get ready for remote deposit capture risk management scrutiny

Banks that haven't paid much attention to the guidance federal banking regulators released earlier this year for managing remote deposit capture risks might want to get busy.

In January the Federal Financial Institutions Examination Council (FFIEC) released guidance for identifying risks and evaluating controls associated with remote deposit capture (RDC). Since then, regulators have been more focused on capital liquidity issues

examining are the FFIEC but that's change. will be more to how manage risks as financial institutions return to profit.



than how banks following guidance, about to Regulators paying attention banks their RDC more

Remote deposit capture allows banking customers to deposit checks from their home or office by scanning a check and transmitting the image to the bank for posting. The process was made possible by the Check 21 Act, legislation implemented in 2004 that allows banks to clear checks based on digital images in lieu of paper.

The FFIEC guidance addresses the core elements of RDC risk management, including assessing legal, compliance and operational risks and mitigation measures. The FFIEC said remote deposit capture can reduce costs and support new products but also introduces new risks.

Many banks reviewed the guidance quickly when it came out and assumed they were in compliance but haven't performed a gap analysis. Large financial institutions may be closer to complying with the FFIEC's RDC guidance because they have the resources, but the guidance expanded the definition of remote deposit capture to any form of deposit document imaging.

Source: Marcia Savage, Site Editor
05 Oct 2009 | SearchFinancialSecurity.com

Don't forget the cleaning crew in your vendor management program

When it comes to their vendor management program, financial institutions often overlook non IT-vendors -- the cleaning crews and other service providers that can pose a real risk to sensitive information.

Banking regulators require financial institutions to have vendor management programs that ensure customer data is protected. However, many banks focus only on IT vendors. That leaves out suppliers like janitors and plant maintenance providers whose after-hours and unsupervised access to office facilities makes them a high risk for stealing confidential information left on desks or in trash cans.

Regulators are looking for an enterprise-wide vendor management program that takes into account all types of vendors.

One example of unchecked risks with non-IT vendors occurred while a consultant noticed evening late one a preschooler, followed by his father, the restroom bank office. It turned out the man was husband of a woman working cleaning and that he and his son regularly brought her dinner to the office. The scenario: a completely unknown entity, the husband, within a secured area and no one from the bank had any idea about it. The bank didn't have any assurances that the cleaning crew was properly vetted or any contractual clauses to govern such a situation.



Continued on Page 2

By overlooking non-IT vendors and not implementing proper security controls, financial institutions run the risk of violating GLBA if the vendor gains unauthorized access to sensitive information. They also are putting customers at risk for identity theft. Other third parties to consider include accounts payable and HR vendors to ensure corporate and employee information is secure.

While physical theft is the main risk with vendors like cleaning services and security guards, there is the chance that criminals could plant a person with technical skills on a cleaning crew to break into computers and steal data. The proliferation of small and cheap storage devices also provides criminals with a way to siphon off data if they can access machines.

Financial institutions need to educate users about shutting down and locking systems during off hours and not writing down passwords, but they also need to deploy technical measures such as controls that prevent someone from plugging a flash drive into a PC.

A good place for banks to start an enterprise-wide vendor management process is with a vendor list from accounts payable. Do a risk assessment on those vendors and decide who should be incorporated into a vendor management program and who you can exclude but it should be noted that you went through that process.

For higher risk vendors, a company may want to verify they're insured or that a confidentiality agreement is in place.

A written vendor management program is a regulatory requirement and regulators will be reviewing banks' programs. Although this year there have been credit situations that are occupying examiners' attention, institutions should not get complacent or lax in thinking that because this year no one looked at it or commented on it that they will get by next year.

Social media: Risk management strategies for financial institutions

The growth of social networking, micro-blogging and collaborative media, such as Facebook, LinkedIn, Twitter and wikis, presents financial institutions, like other businesses, with both challenges and opportunities. Like blogging a few years ago, social media offers businesses a new channel for advertising and customer communications, while employee usage creates various reputational, liability and information security risks (in addition to lost productivity). Enterprises need to adopt a comprehensive social media strategy with policies tailored to the requirements and culture of their business in order to tap the potential and manage the risks of new media.



Financial institutions, however, are not like other businesses, as they have special compliance

requirements for communicating with customers, advertising their products and services, protecting customers and the institution itself from fraud, and managing reputation risk.

Financial institutions should seriously consider whether to even permit employees to make personal use of social media at work. If they do, such use should be consistent with a written Internet use policy that every employee is required to sign and which should explicitly state that violations may result in disciplinary action. Many elements in such a corporate policy will be the same for non-financial businesses -- e.g., no defamatory or harassing content, no posting of third-party copyrighted materials or trademarks, no posting of confidential or proprietary information.

Continued on Page 3



Source: Marcia Savage, Site Editor
05 Oct 2009 | SearchFinancialSecurity.com

Solutions

A financial institution's compliance and information security officers should be prepared to present copies of the corporate Internet use policy and to discuss it in connection with regulatory examinations. Confidential information must specifically include any and all non-public personal information and any associated financial or product eligibility data. As in other corporate policies, unless a social media post is an approved communication or advertisement, the employee should be required to include in or in close proximity to any post that references the financial institution, a conspicuous disclaimer that the post reflects the employee's personal views and not those of the institution.

Because financial regulations require specific disclosures in product advertising, which is also subject to broader scrutiny under the rubric of unfair and deceptive advertising practices, financial institutions -- in addition to requiring a disclaimer -- should prohibit employees from using blogs or social media to provide any description of or statement about the terms, features or availability of products and services, including pricing, rates, rewards, eligibility or decision criteria. Such communications should only be made through authorized channels.

A financial institution should also consider whether to go further and prohibit even generalized comments about its business, since certain comments may reflect adversely on the institution's safety and soundness or reputation or may be taken as misleading or deceptive. If some commentary is permitted, the employee should be required to clearly state his or her affiliation with the financial institution and include a disclaimer that the post reflects his or her personal views.

In addition to evaluating whether and to what extent to permit employee personal usage of social media, financial institutions should integrate social media into their marketing and customer communication strategy, as its rapid and widespread adoption makes it a powerful channel. The danger here is that the very informality of social media -- especially Twitter -- creates an incentive to use it in a spontaneous manner free of the systematic procedures and controls, such as prior legal and compliance review, that apply to direct mail, email and other marketing and communications channels.

Yet precisely because social media is another communications channel, a regulator focused on protecting consumers is likely to apply the same compliance standards. Therefore, all social media posts that represent official statements of the financial institution about its business (e.g., a Facebook page) should

undergo the same prior review process as press releases, including legal review for securities compliance if the company is publicly traded. Posts that include a description of or statement about the terms, features or availability of the institution's products or services, including pricing, rates, rewards, eligibility or decision criteria, should undergo a prior regulatory compliance review.

Where social media is used to communicate with individuals, there are additional compliance, information security and brand management issues. Accordingly, scripts, guidelines and procedures should be developed for handling such customer communication that are integrated with those the institution uses for telephone and email communications and address the following issues.

To combat phishing and spoofing schemes perpetrated through social media where a fraudster impersonates the institution by means of a username or profile incorporating the financial institution's name or trademarks, the institution should adopt an aggressive brand management strategy. This strategy should be coordinated with the institution's information security policy, domain name and trademark protection strategy, and should include the use of in-house resources or a trademark monitoring service to detect potentially harmful or infringing uses of the organization's marks on social media sites and elsewhere on the Internet.

As highly regulated businesses with special obligations to the public, financial institutions must learn to manage the risks of social media before they attract the attention of fraudsters, regulators and plaintiffs' lawyers. With a properly balanced and coordinated social media strategy, financial institutions can reap the benefits of a dynamic new communications channel while avoiding threats to their safety, soundness and the bottom line.

*Source: Compliance And Governance Digest
Andrew M. Baer, Esq., Contributor
June 30, 2009*



**AASYS WILL BE CLOSED ON
THURSDAY, NOVEMBER 26TH
IN OBSERVANCE OF
THANKSGIVING DAY.**

Symantec to launch BackUp Exec System Recovery 2010

Symantec Backup Exec System Recovery 2010 is a simple, cost-effective backup and recovery solution for small businesses that helps minimize downtime and avoid disaster by easily recovering individual data files/folders or complete Windows systems in minutes - not hours or days - even to different hardware, virtual environments, or remote locations.

Key Features

- Backup systems automatically, while you work through scheduled or event-driven backups
- Dissimilar Hardware Recovery with Restore Anyware Technology
- Offsite Backup Copy to FTP location or secondary disk drive for enhanced disaster recovery capabilities
- Seamless physical to virtual (P2V) and virtual to physical (V2P) conversions for VMware, Microsoft and Citrix virtual environments

Key Benefits

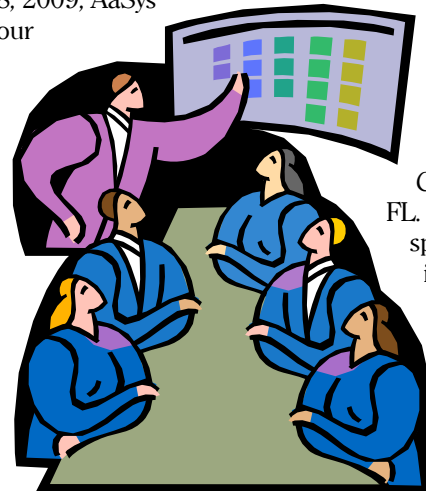
- Manage your business not your backups with proactive data and system protection
- Recover what you need, when and where you need it, including individual files, folders or complete systems in minutes, even to dissimilar hardware or virtual environments
- Replace time-consuming manual and error-prone processes with fast, reliable, automated recovery to dramatically minimize downtime and avoid disaster
- Simplify IT administration by centrally managing backup and recovery tasks for multiple servers across your entire organization (via Backup Exec System Recovery Management Solution)

New Features

- Windows Server 2008 R2 Support
- Granular Restore Option - now included with the core product at no additional cost
- Backup Exec System Recovery Management Solution
- Enhanced Virtual Environment Support
- Support for Exchange 2010

AaSys will host our second User Group Meeting in December!

Our first User Group Meeting was a huge success! This time, we are taking our show on the road. On December 8, 2009, AaSys our



will be hosting second User Group Meeting at Holy Trinity Reception & Conference Center in Orlando, FL. Some of the speakers and topics include Richard Snitzer from the FDIC, Mick Kless of R.I.S.C. Associates will speak about Vendor Compliance

Manager, and Michelle Lucci from Bankers Toolbox will discuss enhanced tools. Of course our resident experts, Miguel Hablutzel, Adrienne DiTunno and Joe DeMartino will also be on hand to answer your questions. We hope to see you there! **IMPORTANT: Don't forget to e-mail us your questions for Richard Snitzer!**

Holy Trinity Reception & Conference Center
1217 Trinity Woods Lane ♦ Maitland, FL ♦ 32751
(407) 331-3036

Directions from I-4 East (Downtown and South Orlando):

Take the first Maitland Exit (90A); immediate right off of the exit onto Sandspur Ramp. Right onto Sandspur Road. Right onto Wymore. Approximately ½ mile straight ahead after traffic light.

Directions from I-4 West (North Orlando):

Altamonte Springs Exit; right off exit. First left onto Wymore. Approximately ¾ mile on the left after overpass.

Signage: Holy Trinity Greek Orthodox Church & Reception Center

Are there topics that you would like to have covered in future newsletters? We are always looking for topics of interest. We welcome all suggestions! To submit a topic, subscribe, or unsubscribe to our distribution list, please email Shama Renée-McIntosh at smcintosh@aaSysgroup.com.