

Solutions

Community Banks: A Financial Bright-Spot?

There are three kinds of banks out there right now: big banks getting big government bucks, small regional banks heavily exposed to real estate that haven't exploded yet, and the third category, which offers a ray of hope: community banks that aren't exposed to real estate and are made more solvent by growing deposits as people focus on saving again. A new report by the Independent Community Bankers of America (ICBA) says things aren't so bad out there for community banks. A poll of nearly 750 institutions showed that 55% have seen an increase in deposits thanks to new customers, and more than 40% are increasing their lending over last year.



April is Community Banking Month!

Every year ICBA, state and regional partners, and community banks across the country celebrate the things that make community banking great. This special observance gives you a chance to tell the public what community banking is all about and to thank the customers who support you. ICBA has made it easy and cost-effective for your bank to participate. With press materials, hints from banks across the country, and turnkey marketing, preparing for Community Banking Month is easy.

Please visit <http://www.icba.org/> for more information.

Community Bank Advantages

- Community banks focus attention on the needs of local families, businesses, and farmers. Conversely, many of the nation's megabanks are structured to place a priority on serving large corporations.
- Unlike many larger banks that may take deposits in one state and lend in others, community banks channel most of their loans to the neighborhoods where their depositors live and work, helping to keep local communities vibrant and growing.
- Community bank officers are generally accessible to their customers on site. CEOs at megabanks are often headquartered in office suites, away from daily customer dealings.
- Community bank officers are typically deeply involved in local community affairs, while large bank officers are likely to be detached physically and emotionally from the communities where their branches are located.
- Many community banks are willing to consider character, family history and discretionary spending in making loans. Megabanks, on the other hand, often apply impersonal qualification criteria, such as credit scoring, to all loan decisions without regard to individual circumstances.
- Community banks offer nimble decision-making on business loans, because decisions are made locally. Megabanks must often convene loan approval committees in another state.
- Because community banks are themselves small businesses, they understand the needs of small business owners. Their core concern is lending to small businesses and farms. The core concern of the megabank is corporate America.





THE INSIDER THREAT: 16 TIPS TO PROTECT CRITICAL DATA

Is 2009 the Year of the Insider Threat? Last August's arrest of a Countrywide employee in California illustrates the potential impact of a single insider with access to sensitive information. The FBI charged the former employee with taking 2 million names and personal information from the mortgage bank and selling them for a profit. This illustrates the need to have monitoring and controls in place, along with an education program to help employees learn about the insider threat as part of an information security awareness program.

Here are 16 practices that will help provide your institution with defensive measures that could help prevent or detect insider incidents:

1. Consider threats from insiders and business partners in your enterprise-wide risk assessments. This is especially difficult for institutions, as the scope of the "insider" stretches out to service providers and vendors.
2. Clearly document and consistently enforce policies and controls. Clear documentation and communication of technical and organizational policies and controls could have mitigated some of the insider incidents, theft, modification and IT sabotage.
3. Institute periodic security awareness training for all employees. Developing a culture of security awareness is only the first step. Employees also need to be aware that individuals, either inside or outside may try to co-opt them into activities counter to the organization's mission.
4. Monitor and respond to suspicious or disruptive behavior, beginning with the hiring process. This should begin even before an employee is hired. Things to look out for include repeated policy violations that may indicate or escalate into more serious criminal activity.
5. Anticipate and manage negative workplace issues. Institutions should carefully review their processes, beginning with pre-employment, employment and termination. Contentious employee terminations must be handled with utmost care, as most insider IT sabotage attacks occur following termination.
6. Track and secure the physical environment. Most institutions are already on top of this issue. Access attempts should be logged and regularly audited to identify violations or attempted violations of the physical space and equipment access policies.
7. Implement strict password and account management policies and practices. Password and account management policies and practices should apply to employees, contractors and business partners.
8. Enforce separation of duties and least privilege. By giving employees only the resources they need to do their jobs, the possibility that one individual could commit fraud or sabotage without cooperation of another individual within the organization is limited.

9. Consider insider threats in the software development life cycle. While this one won't apply to many of the institutions that operate systems but don't develop them, consideration should be made to look into the software development from vendors and core service providers.

10. Use extra caution with system administrators and technical or privileged users. Practice separation of duties or employing the two-man rule for critical system administrator functions.

11. Implement system change controls.

12. Log, monitor and audit employee online actions.

13. Use layered defense against remote attacks. Especially important is disabling remote access and retrieval of company equipment from terminated employees.

14. Deactivate computer access following termination. This should happen quickly, including all physical locations, networks, systems, applications and data.

15. Implement secure backup and recovery processes. Preparation and implementation of a secure backup and recovery process is critical.

16. Develop an insider incident response plan. It is recommended that only those responsible for carrying out the plan need to understand and be trained on its execution.

Source: http://www.bankinfosecurity.com/articles.php?art_id=1257&opg=1
March 9, 2009 - Linda McGlasson, Managing Editor

ATTENTION!

If you are using a third party vendor to perform an internal network assessment, please be sure that they do not perform a password crack analysis. This can compromise the security of your other vendors. AaSys will be happy to perform a password crack analysis at your request.

Please make note of our new remittance address:

**P.O. Box 55
Thonotosassa, FL 33592**

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@aasygroup.com.