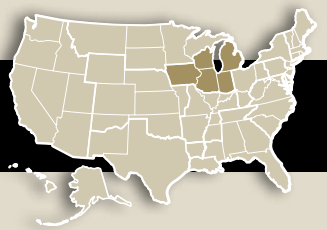
FEDERAL RESERVE SYSTEM

COMMUNITY BANKING
CONNECTIONS®
A SUPERVISION AND REGULATION PUBLICATION

First Quarter 2014



VIEW FROM THE DISTRICT
A Seventh District Perspective — Chicago

Bank Strategies in the New Year: Trends and Examples

by Cathy Lemieux, Executive Vice President, Supervision and Regulation, Federal Reserve Bank of Chicago

Millions of Americans ring in the new year by making resolutions. The promise of turning the calendar spurs many of us to give life to ideas and plans that can make the coming 12 months better than the last. Finances, careers, home improvement, and exercise are at the top of most lists, and for good reason: They have the potential to improve our quality of life and our success in the year ahead.

New Year's resolutions also play out at many financial institutions around this time of year, as banks look to strategic planning to take stock of the past year's performance and recast or recharge their business strategies. Like personal resolutions, these efforts can start out with a full commitment only to fade into old habits. In other cases, these new plans thrive and become ingrained in the culture of the organization.

While the current banking environment has come a long way since the depths of the financial crisis, the new year brings with it a reminder that challenges remain for community-focused financial institutions, from low interest rates to scarce pockets of loan demand. This article discusses some telling stylized examples of banks that found ways to get it right — along with a handful of cautionary examples of strategies missing some key ingredients.

Challenges for Traditional Banks

The very low interest rates of the past five years have been a valuable source of support for the business and consumer borrowers that make up the broader U.S. economy. But low rates continue to be a stiff headwind for traditional banking organizations. With few exceptions, net interest margins have declined every quarter since 2011, most recently to 3.26 percent,[1] well below the 10-year average, which is

[1] Data are from the Federal Deposit Insurance Corporation's Statistics on Banking, available at www2.fdic.gov/SDI/SOB/.

Cathy Lemieux

continued on page 8

INSIDE

Cybersecurity: Part 1 - Demystifying Cyberthreats*

by Qing Liu, Technology Architect, and Sebastiaan Gybels, Risk Management Team Leader, Federal Reserve Bank of Chicago

The U.S. Department of Defense revealed that "at the top of the U.S. intelligence community's 2013 assessment of global threats is cyber, followed by terrorism and transnational organized crime."[1] The severity and impact of cyberthreats have changed the landscape in which governments, corporations, individuals, and, specifically, financial institutions of all sizes and complexities operate.

This article, which is the first of a two-part series, provides background information on cyberthreats and helps individuals working in financial institutions to better understand cyber-related risks and exposures.

What Are Cyberthreats?

According to the U.S. Department of Homeland Security, cyberthreats refer to the possibility of or attempt of gaining unauthorized "access to a device or system or network using a data communication pathway."[2] Seven of the most common cyberthreats or cyber-related risks that community banks have identified and experienced include the following:

- Malicious software, or "malware"
- Distributed denial of service attacks
- Automated clearinghouse (ACH)/payment account takeover
- Data leakage
- Third-party/cloud vendor risks
- Mobile/web application vulnerabilities
- Weaknesses in project management or change management

Who Are the Culprits Behind Cyberthreats?

Cyberthreats can come from numerous sources. The U.S. intelligence community has identified several culprits who are responsible for deliberate cyberthreats, including criminal groups, foreign intelligence services, hackers, insiders, and terrorists. It is important to note that these malicious acts are not only perpetrated by external attackers; in some cases, attacks have originated from employees inside a financial institution.

* This article focuses on the seven most significant cyberthreats or risks currently encountered throughout the financial system. A second article will discuss a risk management framework that can be used to implement controls and evaluate the effectiveness of the cybersecurity measures in both financial institutions and associated third-party vendors.

[1] Cheryl Pellerin, "Cyber Tops Intel Community's 2013 Global Threat Assessment," U.S. Department of Defense, April 15, 2013, available at www.defense.gov/News/newsarticle.aspx?ID=119776.

[2] Industrial Control Systems Cyber Emergency Response Team, "Cyber Threat Source Description," available at http://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions.

Community Banking Connections is published quarterly and is distributed to institutions supervised by the Federal Reserve System. Current and past issues of *Community Banking Connections* are available at www.communitybankingconnections.org or www.cbcfrs.org. Suggestions, comments, and requests for back issues are welcome in writing (editor@communitybankingconnections.org) or by telephone at 800-372-0248.

Editor: **Hilda Guay**
Project Manager: **Minh Farnsworth**
Designer: **Dianne Hallowell**

How Do Cyberattacks Affect Community Banks?

Before the digital age, when somebody robbed a bank, the pool of suspects was "limited to the number of people in the general vicinity of that bank," according to Shawn Henry, the former executive assistant director of the FBI's Criminal, Cyber, Response, and Services Branch.[3] "Today when a bank is robbed digitally … the pool of suspects is limited to the number of people on the face of the earth that have a laptop and an Internet connection, because anybody with an Internet connection potentially can attack any other computer that's tied to the network. So the barrier of entry is relatively low."

Financial institutions not only suffer direct financial losses due to cyberattacks but they also face enormous costs when they are victimized by large-scale data breaches following these attacks. These costs include but are not limited to:

- Investigation and forensic costs
- Customer and partner communications costs
- Public relations costs
- Lost revenue due to a damaged reputation
- Regulatory fines
- Civil claims and legal fees

In the Ponemon Institute's *2013 Cost of Cyber Crime Study*,[4] the median annualized cost of cybercrime in the study's benchmark sample was $9.1 million — an increase from the previous year's median cost of $6.2 million. Not having adequate protection against cybercrimes poses a huge operational risk and potentially places a great financial burden on a community bank.

What Are Cyberthreats and Cyber-Related Risks?

Clearly understanding cyberthreats and their mechanisms is the first step in evaluating the risk exposures to financial institutions. Following is a discussion of seven of the most common cyberthreats and cyber-related risks.

Malware is software that is used to disrupt computer operations, gather sensitive information, or gain access to private computer systems. Malware operates by breaching a bank's network, seeking out weaknesses and points of attack — even in the presence of security controls. Malware infections can occur via physical media, such as USB memory sticks, CDs and DVDs, memory cards, and appliances, or through Internet media, such as drive-by downloads, e-mail attachments, file sharing, pirated software, and phishing. Types of malware include computer viruses, ransomware, worms, Trojans, keyloggers, spyware, adware, botnet, and logic bombs, among others; more information about many of these various forms is provided in the table.[5]

[3] Federal Bureau of Investigation, "FBI's Top Cyber Official Discusses Threat," available at www.fbi.gov/news/videos/fbis-top-cyber-official-discusses-threat.

[4] Ponemon Institute, *2013 Cost of Cyber Crime Study: United States*, available at media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf.

[5] Nader Mehravari, "Cybersecurity Update," CERT Cyber Resilience Center, Carnegie Mellon University, July 16, 2013.

Table: Malware Types

Malware/Tools	Description
Virus	A program that has infected some executable software and, when run, causes a virus to spread to other executables. A virus might corrupt or delete data on a computer, use e-mail programs to infect other computers, or even erase everything on a hard disk.
Ransomware	Malware that restricts access to the computer system that it infects and demands that a ransom be paid to the distributor of the ransomware in order for the restriction to be removed.
Worms	Programs that actively transmit themselves over a network to infect other programs without requiring human involvement.
Trojans	Computer programs that appear to have a useful function, but that also have a hidden and potentially malicious function that evades security mechanisms by, for example, masquerading as a useful program that a user would likely execute.
Spyware	Software that covertly gathers user information through an Internet connection without the user's knowledge for advertising purposes or to steal confidential information.
Botnet	A collection of compromised computers connected to the Internet on which malware is running. Each compromised computer is called a bot. The human controlling a botnet is called a botmaster. Command and control servers are web servers that control the botnet under the direction of a botmaster.
Logic bombs	Programming code intentionally inserted into a software system that will cause a malicious function to occur when one or more specified conditions are met.
Phishing	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information.

continued on page 12

Considerations When Outsourcing Internal Audit at Community Banks

by Cynthia L. Course, CPA, Principal, Federal Reserve Bank of San Francisco

Community banks often use outsourcing arrangements to obtain cost-effective expertise in a variety of areas. Internal audit outsourcing is no exception, with many financial institutions of all sizes outsourcing all or a portion of their internal audit activities to public accounting firms or other professional organizations.

While outsourcing internal audit can provide many benefits to community banks, it is not without risk. Effective boards of directors recognize the risks of such arrangements and take appropriate mitigating actions as part of the outsourcing engagement agreement. This article provides an overview of some of the benefits and risks of outsourcing internal audit at community banks, reviews statutory and regulatory requirements for this practice that apply to community banks, and provides some thoughts on managing an outsourced internal audit function.

Historical Views on Outsourcing Internal Audit

Although outsourcing back-office and technical functions has been a long-standing and accepted practice at many financial institutions, it was not until the 1990s that financial institutions increasingly began to outsource their internal audit functions. Even then, though, there was not universal acceptance of such arrangements.

Twenty years ago, the Institute of Internal Auditors (IIA) wrote in its 1994 paper *A Professional Briefing for Chief Audit Executives: The IIA's Perspective on Outsourcing Internal Auditing* that auditing is best performed by an independent entity that is an integral part of the management structure of an organization. The paper further stated that a competent internal auditing department "can perform the internal auditing function more efficiently and effectively than a contracted audit service."[1]

At the time, the federal banking agencies were more open to outsourced internal audit activities than was the IIA, but they still expressed concerns about certain arrangements. In their 1997 *Interagency Policy Statement on the Internal Audit Function and Its Outsourcing*, the federal banking agencies noted that:

> Such outsourcing may be beneficial to an institution if it is properly structured, carefully conducted, and prudently managed. However, the federal banking agencies have concerns that the structure, scope, and management of some internal audit outsourcing arrangements may not contribute to the institution's safety and soundness. Furthermore, the agencies want to ensure that these arrangements with outsourcing vendors do not leave directors and senior managers with the impression that they have been relieved of their responsibility for maintaining an effective system of internal control and for overseeing the internal audit function.[2]

The IIA came to recognize the value that outsourced internal audit can play in organizations. In 2009, the IIA reconsidered its position, stating in its paper *The Role of Internal Auditing in Resourcing the Internal Audit Activity* that "a fully resourced and professionally competent staff that is a key part of the organization, whether in-house or outsourced, best provides internal audit services."[3] The IIA further acknowledged that the optimal solution for sourcing internal audit varies not only by organization but also for a given organization as the nature of its business activities change over time.

[1] Institute of Internal Auditors (IIA), *A Professional Briefing for Chief Audit Executives: The IIA's Perspective on Outsourcing Internal Auditing*, Professional Issues Pamphlet 94-1, p. 2.

[2] See Supervision and Regulation (SR) letter 97-35, "Interagency Guidance on the Internal Audit Function and Its Outsourcing." SR letter 97-35 was subsequently superseded by SR letter 03-5, "Amended Interagency Guidance on the Internal Audit Function and Its Outsourcing," available at www.federalreserve.gov/boarddocs/srletters/2003/sr0305.htm.

[3] The complete paper is available at http://ow.ly/vl97D.

More recently, in December 2013, the Board of Governors of the Federal Reserve System issued Supervision and Regulation (SR) letter 13-19/CA letter 13-21, "Guidance on Managing Outsourcing Risk."[4] While this guidance applies to all outsourced activities, including internal audit outsourcing arrangements, the letter also refers financial institutions to SR letter 03-5, "Amended Interagency Guidance on the Internal Audit Function and Its Outsourcing," issued in 2003, which directly discusses the outsourcing of internal audit to independent public accounting firms and other outside professionals.[5] Although this amended interagency guidance was issued more than 10 years ago, it remains relevant today.

When considering the outsourcing of internal audit activities, it is important to recognize that there is not a one-size-fits-all solution. While there are many advantages to outsourced internal audit, there are also disadvantages. And, of course, regulatory requirements differ depending on the institution's size and ownership structure.

Advantages of Outsourcing

If conducted in a prudent manner, outsourcing some or all of a community bank's internal audit function has several advantages. First, outsourcing gives community banks access to a level of expertise that may be expensive and impractical to maintain internally. This particularly benefits banks in smaller communities, but it also becomes increasingly important as banks offer new products or services or enter new markets requiring new or expanded controls and broader audit expertise.

Second, outsourcing allows community banks to replace the fixed staffing and overhead costs of employees with the variable cost of consultants. This could be a particularly important consideration when staffing for peak audit periods or for special projects.

Third, the rotation of auditors, which can more easily occur in outsourcing arrangements, minimizes the potential for or appearance of a loss of objectivity, which could occur when internal auditors develop close relationships with bank staff. However, there are disadvantages to this rotation, as discussed below.

Lastly, outsourcing the complete internal audit function allows management to focus on overseeing the outsourced internal audit contract and audit scope and implementing the audit function's recommendations.

Disadvantages to Outsourcing

There are, however, disadvantages to outsourcing some or all of a community bank's internal audit function. First, contracted internal auditors will not have the immediate breadth and depth of familiarity with the banking organization's operations that in-house staff has. In addition, too-frequent rotation of contracted auditors reduces institutional knowledge and creates a continual learning curve that may affect the effectiveness of the outsourced function.

Second, the contracted internal auditor's goals may differ from management's goals, unless communication is open, clear, and continual. For example, some contracted internal auditors may be motivated to suggest additional audit activities to increase their billings. Management teams should consider the advice of the contracted audit firm concerning the proposed audit scope and the banking organization's risk profile and ensure that the final scope of the internal audit remains aligned with the goal of receiving an objective assessment.

Third, both a comprehensive engagement letter and frequent oral and written communications are necessary to avoid misunderstandings. Without a sufficiently descriptive engagement letter, a contracted internal auditor may merely follow the prescribed business plan rather than proactively evaluate and contribute to the improvement of governance, risk management, and control processes.

Finally, if any of these or other internal audit weaknesses materialize as a result of the outsourcing arrangement, a key component of internal control would be weakened, potentially causing an unsafe and unsound operating environment within the banking organization.

Outsourcing to the External Auditor?

In the early days of internal audit outsourcing, some banking organizations believed that the most efficient solution was to outsource internal audit to their external audit firms, arguing that this allowed the external auditor to gain additional knowledge about the banking organization, which could assist in conducting the annual financial statement audit. However, this position was of significant concern to the

continued on page 14

[4] See www.federalreserve.gov/bankinforeg/srletters/sr1319.htm.

[5] See SR letter 03-5.

Mobile Banking Risk Identification and Mitigation

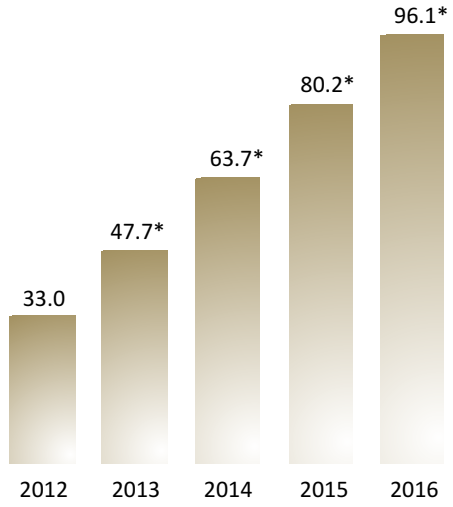
by Jerome F. Combs, Supervisory Examiner, Federal Reserve Bank of Minneapolis

Mobile devices — smartphones and tablets — are easy to use and can be taken almost anywhere. They provide users with easy access to personal and financial data via applications that allow the movement and storage of data locally on the devices and/or allow data to be sent to and stored with a third party. But they can also be lost or stolen, infected with malware, and used as a vehicle for fraud. Even so, smartphones and tablets are here to stay. The way consumers use them may change over time, but it is clear that mobile banking via smartphones and tablets is on trend to grow rapidly in the coming years.

Mobile device software provider Malauzai Software, Inc., released data on August 14, 2013, that confirmed the growing use of mobile banking applications. The report indicated that "For banks and credit unions who have been live a minimum of 12 months, the average month-over-month growth rate is 4.19 percent. The best in class number is 11.56 percent, with several banks and credit unions topping 10 percent. Organic growth is strong and can be attributed to the general growth of mobile smart phone handsets as well as these financial institutions making mobile part of all of their marketing campaigns."[1] In another report based on a 2012 survey of 1,115 U.S. consumers, the Aite Group forecasted that the number of mobile banking users would continue to grow significantly, as shown in Figure 1.[2]

Many community banks recognize the value of mobile banking — it provides them with avenues and opportunities to reach geographically remote or rural markets, to focus on new markets, to innovate, to overcome infrastructure limitations and improve efficiency, to access payment systems, or even simply to retain market share. However, the rapid growth of mobile banking introduces security risk and privacy issues that must be managed. It is critical that banks anticipate and recognize risk in order to protect customers and their own reputation. This article reviews mobile banking risks and risk mitigation solutions, discusses regulatory guidance, and suggests ways to implement mobile banking risk assessment and ongoing risk management strategies at community banks.

Figure 1: Mobile Banking Users in the United States, 2012 to 2016
(in millions)



* These numbers are estimates.

Source: Aite Group

What Is Mobile Banking?

To understand the risks associated with mobile banking, it is necessary to separate mobile banking from the broader arena of mobile financial services and products. Mobile financial services involves the use of a mobile device for transfers (originating wire or automated clearing house (ACH) transactions), marketing, banking, or payments (person-to-person or person-to-business transactions), while mobile banking allows customers of an insured depository institution to conduct banking activities, such as checking balances, receiving account alerts, or making bill payments, through a smartphone or tablet. Mobile financial services, of which mobile banking is a subset,

[1] Malauzai Software, Inc., "Monkey Insights: Mobile Banking Smart Device Usage," August 2013, available at malauzai.com/docs/monkeyinsights_0813.pdf.

[2] Ron Shevlin, "Mobile Banking Forecast: Smartphone and Table Use in the United States" report summary, Aite Group, December 17, 2012, available at www.aitegroup.com/report/mobile-banking-forecast-smartphone-and-tablet-use-united-states.

involve nonbank third parties. As such, this article focuses only on mobile banking because of the unique and ongoing risks faced by financial institutions that offer this service.

Mobile Banking Risk Identification

Providing consumers with the ability to transact banking business using a mobile device — with security settings of the customer's choosing — places an increasing amount of control over sensitive financial data into consumers' hands. The net loss of control over this information makes it more difficult for the bank to assess risks and implement effective risk mitigation strategies.

To understand mobile banking risk, it is important to understand the three most common delivery channels (many institutions offer all three channels to reach the greatest number of customers):

1. Text messaging/short message service (SMS)
2. Mobile-enabled Internet browser
3. Mobile applications

Text Messaging/SMS

SMS, commonly referred to as "texting," is limited in the number of characters used. It is most often used as an alert and inquiry delivery channel. SMS is used to make mobile banking available to users of older cell phones that do not have web browsers or applications. SMS messages are sent in cleartext over widely used telecommunications networks, with no encryption capabilities. Also, the customer's account identifier is stored in an SMS message, which means that there is the possibility of misuse if the phone is lost or stolen. SMS mobile banking users can also be susceptible to receiving misleading or socially engineered messages that could prompt them to reveal account information. Because of the limited utility of older cell phones and the growth of smartphones, the use of SMS for mobile banking is fading.

Mobile-Enabled Internet Browser

Mobile Internet banking via a mobile-enabled Internet browser is an extension of the online banking channel. Customers can navigate to a website on a smartphone or tablet via the embedded browser in much the same way that they can access a site from a personal computer. Although banking from a mobile device using a mobile-enabled Internet browser is open to the same vulnerabilities as banking from a personal computer, it is usually harder to see and use security features on a mobile device.

Mobile Applications

Mobile application banking uses a custom-designed software application installed on a smartphone or tablet that provides for a more user-friendly interface than is possible with either SMS or mobile browser-based banking. As such, this is the fastest growing delivery channel for mobile banking. However, this channel introduces risks that may arise if third parties write the code for these applications, as well as the possibility that the applications can be compromised if customers install rogue, corrupted, or malicious software.

The storage of customer data on a phone or tablet presents the opportunity for misuse if the device is lost or stolen. In addition, likely attacks against mobile banking include fraudulent requests (e.g., phishing e-mails or SMS messages) that appear to require the installation of a new application or security feature from a bank, or malware that can steal credentials by prompting users to type an account number and password.

A good source of information related to mobile security risks is the Open Web Application Security Project (OWASP), a worldwide nonprofit organization focused on improving the security of web application software. It has developed a list of what it views as the top 10 risks arising from the use of mobile applications. Highlights of some of the risks that may be most relevant for community banks are summarized below:[3]

- **Insecure data storage.** Threats include lost or stolen phones or tablets and the possibility of malware gaining access to the device.
- **Weak server side controls.** This pertains to the back-end computers that the mobile banking process needs to use. The security, authentication, and general controls related to these computers need to be strong.
- **Insufficient transport layer protection.** This refers to the lack of data encryption when data travel over public networks.
- **Poor authorization and authentication.** Some mobile applications rely only on unchanging, potentially compromised values for authentication, and some identification data can remain even after data wipes or resets.

[3] The full list of the top 10 mobile application risks is available at www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks.

continued on page 17

Bank Strategies in the New Year: Trends and Examples

continued from page 1

above 4.0 percent. Although a steady drop in funding costs has helped support margins, a steeper simultaneous decline in interest income has challenged community banks' earnings.

The "low for long" rate environment has not translated into robust loan demand nationwide. While there are some bright spots of growth, many banks have struggled to maintain or grow loan portfolios despite holding high levels of deposits.

Competition for "good credits" has led to banks of all sizes competing fiercely to be the lender of choice. In some cases, institutions have responded to weak loan demand by entering specialty or niche markets — such as energy, health care, and equipment financing — in which they previously had little or no presence.

These markets point to commercial and industrial (C&I) lending, which has become a business line of emphasis at many institutions; in some cases, supervisors have seen rising concentrations of C&I loans. Just over a year ago, my colleague Cynthia Course from the Federal Reserve Bank of San Francisco contributed a prescient article to this publication, in which she reminded C&I lenders of the importance of sound risk controls and concentration limits.[2] I encourage bankers who are interested in C&I portfolio growth to read her article.

Another sector showing signs of fierce competition is commercial real estate (CRE), where loan balances are also once again trending upward at some smaller banking organizations following a years-long decline in the wake of the financial crisis. Although construction and land development credits were essentially flat over the past year, as of the third quarter of 2013, loan balances for CRE and multifamily properties rose by 10.7 percent.[3] Federal Reserve data point to growing competition for this business from large financial institutions and other investors,[4] which may tempt some community banks to loosen their underwriting standards.

Knowing Your Strategy — Desk-Side Stories

There are books, consulting firms, and university programs devoted to the finer points of strategic planning. In most cases, these are great resources for community bank managers. However, bankers have a long tradition of learning from one another, and, as they do, they build the institutional wisdom and memory that so often help banks get through tougher times. The following composite stories are telling examples of banks that found ways to get it right through three key themes of good strategic planning:

- Casting a vision with the right people and careful execution
- Attracting and developing expertise at the board level
- Sticking to a well-thought-out plan, evaluating and revising as needed

I hope you find these stories interesting and helpful as you evaluate your own strategy.[5]

The Right People, Thorough Execution. The following examples highlight the importance of laying the risk management groundwork in staffing and capital when casting a new strategic direction.

Consider the example of a community bank grappling with slow economic growth in its local market — in this case a combination of outlying suburban and rural communities. While the large urban center 70 miles down the interstate has put some distance on the financial crisis, its construction activity and tech-focused jobs have yet to provide much help to this bank's local markets. The loan demand among nearby small businesses and farmers by and large results in low-return credits that yield no more than a percentage point or two above mortgage bonds backed by the federal government.

To buttress earnings until the local economy improves, this

[2] Cynthia Course, "Sound Risk Management Practices in Community Bank C&I Lending," *Community Banking Connections*, Fourth Quarter 2012, available at www.cbcfrs.org/articles/2012/Q4/Sound-Risk-Management-Practices-in-Community-Bank-CI-Lending.cfm.

[3] See the Federal Deposit Insurance Corporation's Statistics on Banking, available at www2.fdic.gov/SDI/SOB/.

[4] Board of Governors of the Federal Reserve System, *Senior Loan Officer Opinion Survey on Bank Lending Practices*, October 2013, available at www.federalreserve.gov/boarddocs/snloansurvey/201311/default.htm.

[5] For purposes of confidentiality, each anecdote is a composite sketch of broad supervisory observations. No example included in this article reflects the experience of a single institution.

community bank decided to invest more funds in structured investment products as well as larger loans syndicated by other banks. While the higher yields on these investments were attractive, the bank's board of directors was also aware that these types of loans and investments had been a source of deep losses for other institutions during the most recent financial crisis. The board also paid close attention to a recent report by the U.S. federal banking agencies showing that criticized assets among Shared National Credits (SNCs) held by banks remained elevated at 10 percent of the $3 trillion U.S. SNC portfolio.[6] The agencies' report also called attention to leveraged loans and weakening underwriting practices among SNC participants.

> "Bankers have a long tradition of learning from one another, and, as they do, they build the institutional wisdom and memory that so often help banks get through tougher times."

To round out the new strategy, the board authorized the bank's senior management to set prudent controls for underlying credit risk, growth rates, and balance sheet concentrations. At the same time, the board budgeted funds for the bank to hire two senior staff members — one with experience evaluating and selecting large shared credits, and another with knowledge of structured and complex investment products. The board also adopted a recommendation from the chief financial officer to set concentration thresholds on the amount of investment products relative to capital in which the firm was willing to invest. (For additional discussion of tying strategies to sound capital planning, see Jennifer Burns's insightful article in the Third Quarter 2013 issue of *Community Banking Connections*.[7])

A similar story has played out at some rural community banks focused on agricultural credit and customers. Yet, as the next example shows, banks that shift strategies without sound planning can serve as cautionary cases.

Over the past few years, at one rural bank, the low-interest-rate environment reduced interest income on variable-rate agriculture loans. To diversify business lines and improve profits, the bank's senior management decided to take advantage of opportunities in surrounding counties to fund higher-yielding loans for big-ticket construction equipment and vehicle purchases by businesses. To conserve resources, the chief executive officer (CEO) decided to use existing staff — who did not have a thorough understanding of these types of credits — for these new lending efforts. Before the loans were two years old, asset quality issues arose within the portfolios, and the resulting losses put a strain on the bank's capital. Board meetings now include deliberations for disposing of repossessed vehicles and machinery, the values of which do not cover their associated loan balances.

Beefing Up the Board. The next few examples highlight the importance of an active and engaged board of directors.

In a story familiar to many institutions, a community bank serving an urban area with a mix of businesses and residential neighborhoods spent considerable time triaging the effects of the most recent financial crisis — in this case, asset quality issues among small business loans. After five years of hard work, the bank began exiting what its board of directors had come to call "crisis mode." Capital had been restored, a small portfolio of new loans was performing well, and the neighborhoods the bank serves were showing signs of improving economic conditions. The bank then shifted its attention to loan growth within its CRE portfolio.

To help the bank adopt a forward-looking approach, the six members of the board unanimously decided to recruit two new directors with ties to local business sectors. After a search, the board added the owner of a small but established manufacturing company, as well as a business attorney. To maximize the new directors' contributions, the board also spent some funds to send each one to an educational conference for experienced professionals joining their first bank board of directors.

Two months later, after careful deliberations with the new directors, the board and senior management identified three specific types of local borrowers the bank would target for new

[6] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency, *Shared National Credits Program: 2013 Review*, September 2013, available at www.federalreserve.gov/newsevents/press/bcreg/bcreg20131010a1.pdf.

[7] Jennifer Burns, "Capital Planning: Not Just for Troubled Times," *Community Banking Connections*, Third Quarter 2013, available at www.cbcfrs.org/articles/2013/Q3/Capital-Planning-Not-Just-for-Troubled-Times.cfm.

loans and related business services. The resulting three-year plan included allocating capital relative to distinct borrower risk profiles to ensure the bank's overall capital was managed prudently and to cushion against unexpected losses, as well as dedicating funds to hire a banking professional with experience in choosing and refining underwriting systems. Specific risk controls were established to limit the bank's concentration by loan type and industry. A patient approach to reaching the bank's goals for growth recognized that improved earnings may take more than a few quarters to achieve, allowing management sufficient time to roll out the new strategy. The board also decided to avoid equipment leasing and financing activities after watching a local competitor struggle with asset quality and end-of-lease inventory management issues.

Educating and engaging board members can be valuable in the strategic planning process. Conversely, jumping into a new product or business line without effective challenge from board members can result in future headaches. (For additional discussion of introducing new products or services, see Teresa Curran's helpful article in the First Quarter 2013 issue of *Community Banking Connections*.[8])

For instance, over the past 18 months, the CEO of a large urban community bank noticed an uptick in inquiries from institutions and brokers looking to sell blocks of mortgage servicing rights (MSRs). Although the mortgage servicing industry was previously dominated by very large financial institutions, including Wall Street banks, the financial crisis led to significant shifts within the sector, prompting many organizations to exit the business altogether. Sale prices for MSRs had fallen even as their characteristics made them appear more attractive in the current environment. At the next board meeting, the CEO proposed a purchase of MSRs to help offset weak income from loan interest and fees. The board approved the purchase at that same meeting.

Less than a year later, the MSR business that seemed so promising began to show signs of stress, with implications for the broader institution. The trouble started when more loans defaulted than the bank had forecast, hurting servicing income. A few months later, two borrowers filed lawsuits claiming the bank's newly assembled servicing staff had violated amended consumer protection rules regarding force-placed home insurance and the processing of foreclosure and repossession documents. The bank's general counsel strongly recommended setting aside litigation expenses equal to many months of servicing revenues. Some weeks later, three large local business customers read about the lawsuits in the local media and moved their deposit business to a local competitor.

"Educating and engaging board members can be valuable in the strategic planning process. Conversely, jumping into a new product or business line without effective challenge from board members can result in future headaches."

To be clear, the type of activity the bank engaged in — in this case purchasing MSRs — was not the root cause of the strategy's failure. Rather, the institution's problems were due to the lack of effective review at the board level in questioning potential issues arising from management's proposed strategy, as well as from a failure to lay the appropriate risk management groundwork.

Evaluating and Revising. Finally, it is worth noting the importance of evaluating and at times revising any strategy a bank sets. In today's environment, many community banks that have very traditional commercial banking activities have found themselves reevaluating their strategies, even if these "strategies" are informal and not committed to paper. In the case of the bank discussed in the previous section that grew its CRE portfolio as it exited "crisis mode," the board committed to reviewing its progress and execution every six months. Likewise, at the bank that faced troubles with mortgage servicing, the board of directors recently agreed to carefully review its performance every quarter.

In a final example, a suburban banking institution that serves a cross-section of neighborhoods is long on institutional memory. Although the organization has for years focused on lending to CRE borrowers, it maintained relatively strict un-

[8] Teresa Curran, "Considerations When Introducing a New Product or Service at a Community Bank," *Community Banking Connections*, First Quarter 2013, available at www.cbcfrs.org/articles/2013/Q1/Considerations-When-Introducing-A-New-Product.cfm.

derwriting standards during the most recent financial crisis. It is no coincidence that three of the bank's senior managers began their careers during the savings-and-loan and commercial property crisis that hurt a lot of institutions in the early 1990s.

As less careful competitors retrenched in recent years, opportunities to quickly increase local CRE lending began to present themselves. However, in most of the higher-return opportunities, borrowers were asking for down payments below the bank's historic thresholds. In other cases, would-be borrowers were seeking credit to purchase properties they did not intend to occupy themselves — another loan feature that fell outside the bank's existing underwriting systems. After presenting these new opportunities to the board, the directors decided to turn down 90 percent of the new opportunities. The board made exceptions for three relatively small loans to long-time customers but set aside separate capital to isolate the risk to the rest of the institution. New risk management controls allow senior management to propose additional nonconforming loans, but they must be approved by the full board, not just the bank's loan committee.

Conclusion

Given today's difficult operating environment, many banks are understandably reevaluating their strategies to remain competitive and profitable. The new year is the perfect time to review performance and set resolutions for the year ahead. While challenges to our nation's community banks are stiff, these examples demonstrate that success is possible if banks have involved boards of directors and well-planned strategies supported by the right staff, capital, and controls. They represent the kinds of decisions that can make for a promising year ahead. ■

D.C. UPDATES

Janet Yellen succeeded Ben Bernanke as Chair of the Board of Governors of the Federal Reserve System on February 3, 2014. Prior to becoming Chair, Yellen served as Vice Chair of the Federal Reserve Board since 2010 and was president and chief executive officer of the Federal Reserve Bank of San Francisco from 2004 to 2010. Chairman Bernanke served two terms totaling eight years, from 2006 to 2014. During his tenure, he supported a number of initiatives to enhance communication with community banks, including the establishment of this publication, which featured a conversation with him in the inaugural issue: www.cbcfrs.org/articles/2012/Q3/conversation-with-Bernanke.cfm.

Governor Sarah Bloom Raskin resigned from the Federal Reserve Board on March 13, 2014. Governor Raskin was confirmed by the U.S. Senate to be the deputy secretary of the U.S. Department of Treasury. She provided strong leadership in ensuring that the Federal Reserve's supervisory program for community banks is effective and that supervisory policies and guidance are applied appropriately and in a proportionate manner to community banking organizations. Governor Raskin was a member of the Board's subcommittee that makes recommendations about matters related to community and regional bank supervision and regulation. That subcommittee remains actively engaged in matters affecting community banks following her departure.

The Federal Reserve Board, along with other federal financial regulatory agencies, approved an interim final rule authorizing interests in certain collateralized debt obligations backed primarily by bank-issued trust preferred securities on January 14, 2014. This interim final rule permits banking entities to retain interests in certain obligations under section 619 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, known as the Volcker rule. The Board's press release announcing the interim final rule is available at www.federalreserve.gov/newsevents/press/bcreg/20140114b.htm.

Cybersecurity: Part 1 - Demystifying Cyberthreats *continued from page 3*

Distributed denial of service (DDoS) attacks, which have been used extensively since 2012, repeatedly target major U.S. banking websites and services, making the institutions' online services unavailable. The wave of DDoS attacks has a broad range of targets, including large regional and community banks as well as credit unions and technology service providers.

DDoS attacks occur when an attacker leverages a number of computers from various locations to send simultaneous requests to a target computer or website. In other words, the attack has the same effect as if millions of users were simultaneously opening a web browser and going to the same web page. The overwhelming flood of requests to the web server or computer network is intended to cause a shutdown or failure to handle the requests of legitimate users, much like a rush-hour traffic jam on a freeway. The goal of a DDoS attack is usually to limit, disrupt, or prevent access to a particular network resource or web service. Although these attacks pose limited financial risk, they clearly create reputational risks for the affected banks, since their customers may experience a slower-than-usual connection or be unable to access online banking services.

ACH/payment corporate account takeover is a type of identity theft in which cyberthieves gain control of a business's bank account by stealing the business's valid online banking credentials through various methods. A classic example of this type of cybercrime was an ACH/account takeover at a community bank. To initiate the attack, several e-mails from an industry group were circulated to an employee of one of the bank's commercial customers. The e-mail stated that a transaction had not cleared properly and that the reader should click on a link to resolve the problem. As soon as the e-mail link was clicked, hackers were able to install a keylogger — a program that tracks a user's activity and allows access to the commercial customer's bank accounts. After gaining the commercial customer's online banking passwords, the perpetrators directed the bank to process a money transfer to an offshore account. The commercial customer received a confirmation of the transaction and immediately called the bank to stop it, but it was too late — the money was gone.

Data leakage is the unauthorized transmission of data or information from within an organization to an external destination or recipient. This can be executed electronically or through a physical method. The data leakage can be intentional and malicious, or unintentional and inadvertent.

According to the SANS Institute, data leakage is categorized into four types: the most common is customer data, at 73 percent; then confidential information, at 15 percent; and finally intellectual property and health records, each at 8 percent.[6] Of all data leakage incidents, 52 percent are from internal sources, compared with the remaining 48 percent by external hackers. Internal data leakage is significant because it is mainly caused by a lack of employee oversight and weak business processes. Internal data leakage may occur through various communication channels such as instant messaging, e-mail, web mail, web logs/wikis, malicious web pages, removable media/storage devices, hard copy, cameras, and unsafe file transfer protocols, among other methods. External data leakage is mainly triggered by external hackers using social engineering or malware, phishing, or taking advantage of web application vulnerabilities.

Third-party/cloud vendor risks will expose a financial institution to risks that are outside of its immediate control; therefore, the financial institution has to rely on due diligence in the contract and monitoring of the service provided, rather than being able to manage the risk in-house. Third-party/cloud vendors provide critical services to financial institutions such as core data processing, payment processing, credit card processing, mobile banking, and ensuring business continuity. Banks' sensitive data are often handled or stored by third-party vendors and their subcontracted companies for business purposes. When a data breach occurs at these vendors, it can directly jeopardize the confidentiality, integrity, and availability of the financial institution's data. It is important to note that a bank can outsource operational functions to third parties, but the bank will remain the owner

[6] Peter Gordon, SANS Institute, *Data Leakage — Threats and Mitigation* (2007), available at www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-mitigation-1931?show=data-leakage-threats-mitigation-1931&cat=awareness.

of bank data and, therefore, is ultimately responsible. Additionally, when a cyberattack targets a service provider, the attack might not be directed at a specific financial institution. This means that whenever the cyberattack affects the service provider's environment, it may impact the operations of several banks that are using the same operating environment. Therefore, the concentration of services by third-party vendors can negatively impact multiple banks even when the affected banks are not the direct targets of a cyberattack.

Mobile/web application vulnerabilities are the weaknesses or flaws that reside in a mobile application, smartphone, or Internet-facing web server. To expand business and attract new customers, more financial institutions are leveraging innovative technology, such as mobile payment applications on smartphones or tablets.[7] The mobile platform (both smartphone and mobile applications) is still maturing, and it does not always provide the same level of security features that are typically found on a desktop or laptop. As a result, a hacker can use tools to gain access to and exploit the mobile platform, gain sensitive information stored or processed by mobile applications on the customer's mobile device, or take over controls of a payment web server.

[7] For more information about the risks involved with mobile banking and how to mitigate those risks, see Jerome F. Combs, "Mobile Banking Risk Identification and Mitigation," *Community Banking Connections,* First Quarter 2014.

Weaknesses in project management or change management can directly expose a bank's core financial systems or sensitive data. Banks use project management and change management to address changes in the information technology infrastructure to support current business processes or integrate new technology or products. Banks also have change management processes in place to update existing systems or products, patch the vulnerabilities in legacy products, and manage the life cycle of software and hardware. Weaknesses in project management or change management processes can undermine policies and procedures, delay vulnerability discovery and mitigation, and expose bank systems or sensitive data to intruders.

Conclusion

Cyberthreats and cyberattacks have increased dramatically over the past several years. They have exposed sensitive personal and business information, disrupted the critical operations of institutions, and imposed high costs on the economy and business operations. That is why it is imperative that financial institutions stay informed about the continuously changing forms of cyberthreats and develop appropriate, cost-effective controls to safeguard their businesses. Part two of this article will expound upon the four control pillars of a general cybersecurity framework: risk assessment; policy, procedure, and control implementation; governance and monitoring; and resiliency and incident response. ■

REGULATORY RECAP

Supervision & Regulation (SR) & Consumer Affairs (CA) Letters

The following SR and CA letter that has been published since the last issue of *Community Banking Connections* applies to community banking organizations. In general, letters that contain confidential supervisory information are not included. All SR letters are available by year at www.federalreserve.gov/bankinforeg/srletters/srletters.htm and by topic at www.federalreserve.gov/bankinforeg/topics/topics.htm. A complete list of CA letters can be found at www.federalreserve.gov/bankinforeg/caletters/caletters.htm.

SR Letter 14-2/CA 14-1, "Enhancing Transparency in the Federal Reserve's Applications Process"

Considerations When Outsourcing Internal Audit at Community Banks *continued from page 5*

Securities and Exchange Commission (SEC), the American Institute of Certified Public Accountants (AICPA), and the federal banking regulatory agencies, all of which believed that outsourcing internal audit to the external auditor had a high potential to compromise the external auditor's independence.

As noted earlier, in 2003, the federal banking agencies issued an Interagency Policy Statement on the Internal Audit Function and Its Outsourcing."[6] This statement superseded the 1997 policy statement to align supervisory policy with the prohibitions on internal audit outsourcing imposed by the Sarbanes–Oxley Act of 2002 and SEC regulations. Part III of the 2003 policy statement provides a detailed discussion of the regulatory rules and guidance in this area.

Highlights of the various rules, regulations, and policies concerning the outsourcing of internal audit at financial institutions are discussed below. The decision tree in the figure on this page shows how community banks can put these requirements in context.

Federal Deposit Insurance Act

The independence of the external auditor is important for financial institutions of all sizes but is of particular importance to a financial institution with total consolidated assets of $500 million or more, regardless of whether it is a public company. Section 36 of the Federal Deposit Insurance Act and associated regulations require every insured depository institution with $500 million or more in total consolidated assets to obtain an annual audit of its financial statements by an independent public accountant.

Part 363 of the Federal Deposit Insurance Corporation's regulations (12 CFR) states that the independent public accountant must comply with the independence standards and interpretations of the AICPA, the SEC, and the Public Company Accounting Oversight Board (PCAOB). Further, to the extent that any of the rules issued by these organizations is more or less restrictive than the corresponding rule in the other independence standards, the independent public accountant must comply with the more restrictive rule.[7]

Thus, nonpublic banking organizations with $500 million or more in total consolidated assets are also subject to the SEC's independence requirements for external auditors, discussed below. Furthermore, the federal banking agencies have long encouraged banking organizations with less than $500 million in total consolidated assets to adopt an external auditing program that includes an annual audit of its financial statements by an independent public accountant and to follow the SEC's internal audit outsourcing prohibition (also discussed below).

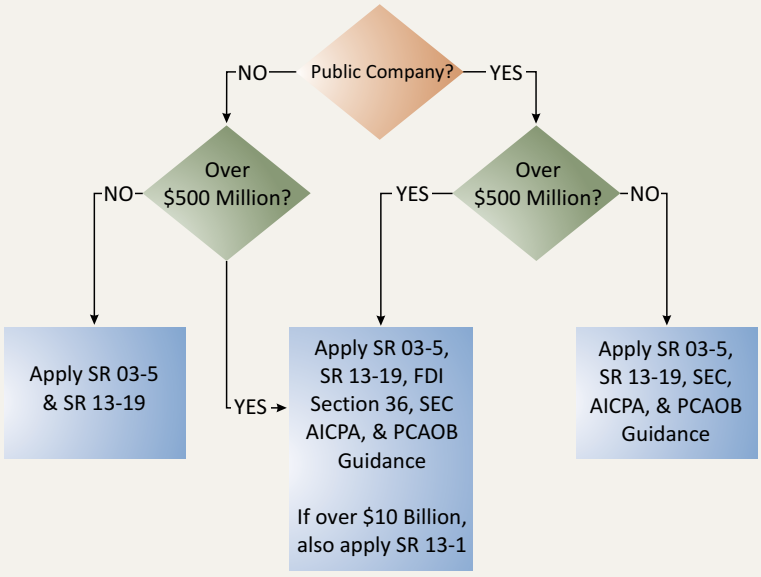
SEC Guidance

The Sarbanes–Oxley Act of 2002 was intended to protect investors by improving the accuracy and reliability of corpo-

[6] See SR letter 03-5.

[7] See "Part 363 — Annual Independent Audits and Reporting Requirements," 12 CFR section 363, available at www.gpo.gov/fdsys/pkg/CFR-2013-title12-vol5/pdf/CFR-2013-title12-vol5-part363.pdf.

Applying Guidance on Outsourcing Internal Audit



rate disclosures made pursuant to securities laws.[8] Title II of the act, which addresses auditor independence, applies to companies with securities registered with the SEC or a federal banking agency or companies that are required to file reports with the SEC (that is, "public companies"). Section 201(a) of the act amended section 10A of the Securities Exchange Act of 1934, prohibiting a public company's external auditor from also performing eight specific services, one of which is internal audit outsourcing services.

In 2003, the SEC updated its rules to state that:

> An accountant is not independent if, at any point during the audit and professional engagement period, the accountant provides … any internal audit service that has been outsourced by the audit client that relates to the audit client's internal accounting controls, financial systems, or financial statements, for an audit client unless it is reasonable to conclude that the results of these services will not be subject to audit procedures during an audit of the audit client's financial statements.[9]

The SEC's final rule permits, with audit committee approval, outsourcing of internal audit that (1) is not related to the audit client's internal accounting controls, financial systems, or financial statements or (2) will not be subject to audit procedures during an audit of the audit client's financial statements. However, banking organizations that are public companies and their external auditors should exercise caution when entering into such arrangements and should ensure that they are permissible under any applicable rules or guidance.

AICPA Guidance

The AICPA addresses the appropriateness of outsourcing internal audit to an external auditor in its Code of Professional Conduct. Interpretation No. 101-3, "Nonattest Services," under Rule 101, *Independence*, starts with the premise that:

> Assisting the client in performing financial and operational internal audit activities would impair independence, unless the member takes appropriate steps to be satisfied that the client accepts its responsibility for designing, implementing, and maintaining internal control and directing the internal audit function, including the management thereof.[10]

Interpretation No. 101-3 goes on to provide specific examples of the management responsibilities that cannot be delegated and describes activities that, if performed as part of an internal audit engagement, would impair independence. The AICPA could not, however, anticipate all possible conflicts; therefore, the guidance is not all-inclusive and, in some instances, may be subject to interpretation.

PCAOB Guidance

On April 26, 2006, the SEC approved the PCAOB's initial rules governing independence.[11] The PCAOB's rules have been subsequently amended and clarified, with SEC approval; they remain generally consistent with the SEC's rules and will not be discussed further here.

Other Considerations for Community Banks

The federal banking agencies have issued additional guidance that many community banks may find particularly relevant.[12]

Nonpublic Community Banks with Less Than $500 Million in Total Assets

As noted above, the federal banking agencies have long encouraged banking organizations with less than $500 million in total consolidated assets to adopt an external auditing program that includes an annual audit of its financial statements by an independent public accountant and to follow the SEC's internal audit outsourcing prohibition.[13] However, the federal

[8] See Sarbanes–Oxley Act of 2002, Public Law No. 107–204, 116 Stat. 745 (2002), available at www.gpo.gov/fdsys/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf.

[9] See 17 CFR section 210.2-01 (c)(4)(v), available at www.gpo.gov/fdsys/pkg/CFR-2013-title17-vol2/pdf/CFR-2013-title17-vol2-sec210-2-01.pdf.

[10] See the AICPA's Code of Professional Conduct, available at www.aicpa.org/research/standards/codeofconduct/pages/et_101.aspx.

[11] See Section 3 — Professional Standards of the PCAOB, including the rules related to independence and communication with the audit committee concerning independence, available at pcaobus.org/rules/pcaobrules/pages/section_3.aspx.

[12] In addition to issuing guidance, the federal banking agencies participated in the development of a June 2012 paper by the Basel Committee on Banking Supervision titled "The Internal Audit Function in Banks." While this paper sets forth principles that banks may find to be relevant depending on their size, complexity, and risk profile, it does not establish requirements for U.S. banking organizations and is not a substitute for U.S. policies and guidance on internal audit and its outsourcing. The paper is available at www.bis.org/publ/bcbs223.pdf.

[13] See, for example, SR letter 99-33, "Interagency Policy Statement on External Audits of Banks With Less Than $500 Million in Total Assets," available at www.federalreserve.gov/boarddocs/srletters/1999/SR9933.htm.

banking agencies believe that a smaller nonpublic banking organization with less complex operations and a limited staff can, in certain circumstances, use the same accounting firm to perform both an external audit and some or all of the organization's internal audit activities.[14]

This does not, however, give banks carte blanche permission to outsource internal audit to the external auditor. The 2003 interagency policy statement describes a nonexclusive set of circumstances in which outsourcing to the external auditor may be acceptable. In these cases, the federal banking agencies expect the audit committee and the external auditor to pay particular attention to preserving the independence of the separate audit functions. The audit committee should document that it has preapproved the internal audit outsourcing to the external auditor and that it has considered the independence issues with this arrangement. Furthermore, the banking organization's board of directors and management cannot abdicate their oversight responsibilities for the internal audit function.

Community Banks Approaching $10 Billion in Total Assets

In January 2013, the Federal Reserve issued *Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing*.[15] This guidance was directed at financial institutions with more than $10 billion in total consolidated assets and does not apply to community banks, which the Federal Reserve generally defines as those with $10 billion or less in total consolidated assets. However, management of larger community banks approaching this threshold should be aware of this guidance and be prepared to comply with it if they grow beyond the $10 billion threshold, as it builds on the 2003 guidance and discusses enhanced internal audit expectations for larger firms.

Managing the Relationship with the Outsourced Internal Audit Company

Regardless of whether internal audit is outsourced to the external auditor or a different firm, a community banking organization's board of directors and management must actively oversee the internal audit function, just as they are expected to oversee the relationship with any third-party vendor.

As noted previously, the Federal Reserve recently issued supervisory guidance on managing the risks of any outsourced activities. This guidance discusses the risks of outsourcing activities to third parties, board of director and senior management responsibilities, and appropriate service provider risk management programs.[16] In summary, the board of directors and management must ensure that the outsourced activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations. In addition, relationships with outsourced internal auditors are subject to the same risk management, security, privacy, and other laws, regulations, and policies that a financial institution would be expected to abide by if the activity were conducted in-house.

To better ensure the appropriate oversight of and accountability by the outsourced internal auditor, the banking organization should have a written contract or engagement letter that sets forth the full details of the rights and responsibilities of each party. Both SR letter 13-19/CA letter 13-21 and section 1010.1 of the Federal Reserve's *Commercial Bank Examination Manual* provide more detailed information on typical contractual provisions, which include assessing the outsourced internal auditor's competence, independence, and objectivity; managing the outsourced internal auditor relationship; and developing appropriate contingency plans to ensure the continuity of internal audit activities.[17]

Summary

Outsourcing internal audit can provide several advantages for community banks, but it is not without risk. As with all banking decisions, when deciding whether to start, modify, or continue an internal audit outsourcing arrangement, effective boards of directors and management teams consider both the regulatory expectations and the operational aspects of the arrangement to ensure that their financial institutions continue to operate in a safe and sound manner and in compliance with all laws and regulations. ■

[14] For more information, see page 13 of the "Interagency Policy Statement on the Internal Audit Function and Its Outsourcing" that is attached to SR letter 03-5, available at www.federalreserve.gov/boarddocs/srletters/2003/sr0305.htm.

[15] See SR letter 13-1/CA letter 13-1, "Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing," at www.federalreserve.gov/bankinforeg/srletters/sr1301.htm.

[16] See SR letter 13-19/CA letter 13-21, "Guidance on Managing Outsourcing Risk."

[17] See the Federal Reserve's *Commercial Bank Examination Manual*, available at www.federalreserve.gov/boarddocs/supmanual/cbem/cbem.pdf.

Mobile Banking Risk Identification and Mitigation

continued from page 7

Mobile banking introduces new security risks, threats, and challenges to financial institutions. Although no mitigation scheme can completely eliminate risk, banks should develop practices to effectively safeguard the mobile banking process. By staying abreast of security risks and developing effective mobile banking practices, a bank can reduce and better manage its legal, operational, and reputational risks.

Mobile Banking Risk Mitigation

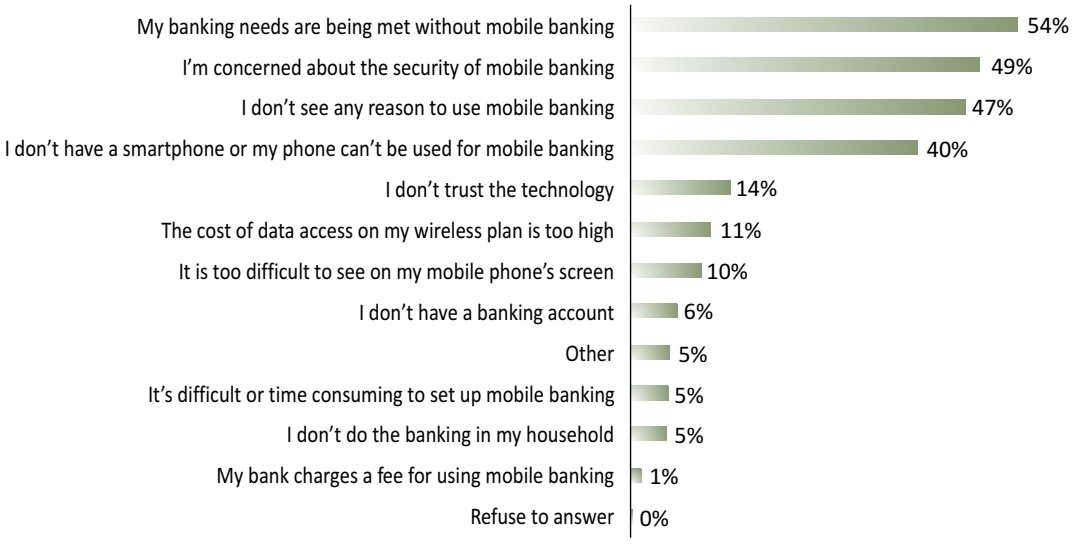
With the convenience and rapid promotion of mobile banking, it may seem puzzling that many customers are still reluctant to embrace it. In a March 2013 Federal Reserve System survey,[4] consumers were asked "What are the main reasons you decided not to use mobile banking?" The most commonly cited reason was security, such as data loss, fraud, identity theft, and other risks (Figure 2).

A careful reading of the OWASP list of risks faced by banks offering mobile banking reveals that many of these risks are aligned with the risks that are perceived by their customers, as noted in Figure 2. Accordingly, the actions a bank takes to mitigate its risk could positively influence customers' sense of security and their willingness to adopt this service.

As part of its Mobile Security Project, OWASP has also outlined suggested risk mitigation solutions — a list of its top 10 mobile controls — that address the mobile risks outlined above.[5] The controls are discussed below from the perspective of the bank providing mobile financial services. For example, highlights of some controls a bank should consider when having an application developed for mobile banking include the following:

- **Identify and protect sensitive data on the mobile device.** Store sensitive financial and consumer data on another computer instead of on the mobile device. If data are stored on the device, use strong encryption technology provided by a trusted source.
- **Ensure that sensitive data are protected while in transit.** Assume nothing is secure. Mobile banking applications should enforce the use of an end-to-end secure channel such as secure sockets layer/transport layer security (SSL/TLS) and use strong encryption.
- **Implement user authentication, authorization, and session management correctly.** Require appropriate-strength user authentication, for example, multifactor versus strong authentication. Physical tokens or voice, fingerprint, or behavioral authentication factors may be appropriate.
- **Secure data integration with third-party services and applications.** Ensure that mobile banking applications

Figure 2: What Are the Main Reasons for Deciding Not to Use Mobile Banking?*



* n=1,709

Source: Consumers and Mobile Financial Services 2013, Board of Governors of the Federal Reserve System, March 2013

[4] See www.federalreserve.gov/econresdata/mobile-devices/files/consumers-and-mobile-financial-services-report-201303.pdf.

[5] The full list of the top 10 mobile controls is available at www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_Ten_Mobile_Controls (May 22, 2013).

and code are tested, come from a reliable source, have supported maintenance, and have no back-end malware (for example, Trojans).

Mobile Banking Risk Assessment

Once bank management understands the risks posed by mobile banking and the potential strategies for mitigating those risks at a high level, the final step in the process is to apply those general concepts to the specific products and services offered by the bank. This begins with completing a risk assessment based on bank-specific factors. To complete an effective risk assessment, bank management should:

- Understand the network architecture and mobile banking technology solution(s) being used.
- Know how the mobile banking application is designed, understand what features are being used, and be aware of the threats to the application.
- Identify the wireless transmission protocols and data transmission media being used.
- Understand what data the application stores and processes, as well as how this information is stored.
- Know the methods of attack to which the application is vulnerable and which are the most common. Identify controls to prevent attacks and/or data loss.
- Have a robust vendor management process. If a third party (or parties) is involved in offering mobile banking, complete a thorough due diligence to understand all the preceding risk assessment elements as they apply to that third party.

One possibility is to use a data-centric approach to risk assessment and ongoing risk management. Data discovery and classification are two essential initiatives that lay the foundation for protecting data no matter where this information resides. If a financial institution does not know what kind of data it has or where they reside, it cannot apply the appropriate policies and controls to protect this information.[6] This especially applies to mobile banking and the risks and controls discussed in this article. The following table is a simple data classification chart that a bank can fill out that could be used to identify critical data and associated control requirements based on the implementation of a mobile banking solution.

Table: Data Classification and Control Requirements

Type	State	Location	Control Requirements
Public	At Rest	Internal	
Public	At Rest	External	
Public	In Motion	Internal	
Public	In Motion	External	
Bank Private	At Rest	Internal	
Bank Private	At Rest	External	
Bank Private	In Motion	Internal	
Bank Private	In Motion	External	
Customer Private	At Rest	Internal	**On Device (application) –** Sandboxed/isolated application and storage; strong encryption technology (e.g., triple data encryption); no data storage at all
Customer Private	At Rest	External	**Third Party (service provider) –** Strong physical controls; strong logical access controls; strong encryption technology (i.e., disk encryption, file system encryption), strong security policy
Customer Private	In Motion	Internal	**On Device (application) –** Restricted movement between applications
Customer Private	In Motion	External	**Public Network (Internet) –** Strong encryption technology (e.g., virtual private network, secure sockets layer)

For example, consider a financial institution that implements mobile banking and uses a mobile banking application provided by a third-party vendor. A customer will use a mobile device, but the actual device and operating system will not be known by the financial institution. What is known is that the customer's private data will be in motion on a public network between the device and the vendor (that is, this information will be located externally). The customer's private data will rest in storage at the vendor (also located externally).

Mobile Banking Risk Controls

Based on information provided in this article, what control

[6] *SC Magazine* Vendor Webcast, "Rethink Data Classification: Identify Your Data, Know Your Data," September 19, 2013, available at www.scmagazine.com/rethink-data-classification-identify-your-data-know-your-data/article/311972/.

requirements should a bank consider? The answer depends on the type of mobile banking technology being implemented. See the table on the previous page for sample requirements. These are samples only; specific mobile banking implementations and risk assessments may indicate less or more controls.

Options to consider include a secure end-to-end delivery channel on the public network, strong authentication on the device, and strong secure mobile application coding and testing standards for the mobile banking application. If a financial institution cannot meet its controls requirements (including assessment of the controls used by a vendor) at any point, a reassessment is necessary. A financial institution should be able to complete an assessment and provide ongoing risk management by answering four critical questions:

- **Where is it (for example, data type, hardware, software, and process)?** An effective risk assessment process should help answer this question.
- **Who owns it (for example, data type, hardware, software, process, and policy)?** It is critical to assign ownership in order to establish responsibility and accountability.
- **How do you know?** Is there a significant security gap? Are controls working effectively? Are they the right controls? Effective risk assessment and audit processes help answer these questions.
- **What does "normal" look like?** Ensure that monitoring and reporting processes related to data flow and transactions are in place in order to effectively identify abnormal behavior that could indicate malicious activity.

Following this type of process will help ensure that control gaps are identified, action plans to mitigate gaps are developed, and residual risk is acceptable. This process also provides for effective audit validation and feedback related to the intended control environment, leading to a safer and more successful implementation.

Conclusion

Whether it is because of demand from customers or a desire to enter new markets, many community banks are beginning to offer mobile financial services to their customers. As with all new products, bankers need to understand the mobile banking environment being used and the associated risks. Effective risk identification and implementation of mitigation controls and processes based on the data type, state, and location are key to achieving this objective. With the proper strategy and risk management elements in place, both the bank and its customers should experience a safer mobile banking environment.[7] ■

[7] For a broader discussion about adding new services, see Teresa Curran, "Considerations When Introducing a New Product or Service at a Community Bank," *Community Banking Connections*, First Quarter 2013, available at www.cbcfrs.org/articles/2013/Q1/Considerations-When-Introducing-A-New-Product.cfm.

Regulatory Guidance for Mobile Banking

In addition to sources of information from industry groups and associations, regulatory guidance that is pertinent to mobile banking is also available. While not as technical in nature as the OWASP guidance, it nevertheless provides support and direction related to the same control areas. Related guidance includes:

Federal Reserve Supervision and Regulation (SR) Letters:[a]

- SR letter 13-19/CA letter 13-21, "Guidance on Managing Outsourcing Risk"
- SR letter 11-9, "Interagency Supplement to Authentication in an Internet Banking Environment"
- SR letter 05-19, "Interagency Guidance on Authentication in an Internet Banking Environment"
- SR letter 01-15, "Standards for Safeguarding Customer Information"
- SR letter 98-9, "Assessment of Information Technology in Risk-Focused Frameworks for the Supervision of Community Banks and Large Complex Banking Organizations"

Federal Financial Institutions Examination Council (FFIEC) Information Technology Booklets:[b]

- Information Security
- Outsourcing Technology Services
- Business Continuity Planning
- E-Banking
- Audit

[a] SR letters are available at www.federalreserve.gov/bankinforeg/srletters/srletters.htm.
[b] FFIEC IT booklets are available at ithandbook.ffiec.gov/it-booklets.aspx.

FedLinks
Connecting Policy with Practice

FedLinks: Connecting Policy with Practice is a single-topic bulletin prepared specifically for community banks and bank holding companies with total assets of $10 billion or less. Each bulletin provides an overview of a key supervisory topic; explains how supervisory staff members typically address that topic; highlights related policies and guidance, if applicable; and discusses examination expectations as appropriate at community banks. *FedLinks* is not intended to establish new supervisory expectations beyond what is already set forth in existing policies or guidance, but rather to connect policy with practice.

A *FedLinks* bulletin was recently released in February 2014:

"Servicemembers Civil Relief Act" provides an overview of Federal Reserve examiner expectations when reviewing the fundamental elements of a bank's Servicemembers Civil Relief Act compliance program.

This bulletin, and others like it, can be found online at www.cbcfrs.org/fedlinks.cfm.

By subscribing to *FedLinks* bulletins at www.cbcfrs.org/subscribe.cfm, you will receive an e-mail notification when new bulletins become available.

Connecting with You

What banking topics concern you most? What aspects of the supervisory process or the rules and guidance that apply to community banks would you like to see clarified? What topics would you like to see covered in upcoming issues of *Community Banking Connections*?

With each issue of *Community Banking Connections*, we aim to highlight the supervisory and regulatory matters that affect you and your banking institution the most, providing examples from the field, explanations of supervisory policies and guidance, and more. We encourage you to contact us with any ideas for articles so that we can continue to provide you with topical and valuable information.

Please direct any comments and suggestions to www.cbcfrs.org/feedback.cfm.

100 YEARS™
FEDERAL RESERVE SYSTEM

Scan with your smartphone or tablet to access *Community Banking Connections* online.

CONNECTIONS