20 Questions the FFIEC Wants Your Directors to Answer about Cybersecurity Risks

By Charles Cheatham, SVP & General Counsel, BankOnIT
The FFIEC recommends that all boards and CEOs should consider 20 questions regarding cybersecurity. Can your directors answer these questions?

Each of the 20 questions that the FFIEC recently released is analyzed in this document. Ideally, CEOs and board members should be able to answer all of these questions regarding cybersecurity. (If CEOs and directors cannot answer these questions, they may not have a strong enough understanding of the security risks that the bank is taking by conducting operations in the current manner—and how to mitigate those risks. A bank may need to increase the amount of information being provided to its directors. The board, in turn, may need to give increased attention to enhancing security in light of that increased information reporting.)

“4 out of my 8 directors don’t even own a computer”—$300 million community bank president.

What response would your directors give if examiners asked them about your bank’s technology risk? Directors and executive management are well-versed in reviewing credit risk and interest rate risk, but what about technology risk?

Does your bank have stronger cybersecurity protections than Sony Pictures or Target? Could your board explain in what areas your bank’s information is strongly protected—and what aspects of your business still may have some important security vulnerabilities?

The FFIEC also recommends participating in technical information sharing services concerning emerging cybersecurity risks. However, for banks to benefit from this, they must have people who understand what the information is telling them. These people also must have ability and time to implement measures to address the ever-increasing risks as they appear.

“We are focusing in particular on community banks … it is very likely that hackers will turn their attention to community banks”—Thomas Curry, Comptroller of the Currency & FFIEC Chairperson

Technology is changing rapidly and the regulatory risk is growing along with the technical risk. Examiners expect banks to make continuing progress in strengthening information security. How will your bank keep up with the rapid changes in technology and accompanying risks?

“Cybersecurity is no longer just an issue for the IT department. Instead, it needs to be engaged at the very highest levels of corporate management. Cybersecurity has become an issue of the highest importance not only at the FDIC, but for the FFIEC and its member agencies as well as the federal government as a whole.”—Martin J. Gruenberg, FDIC Chairman
What the FFIEC Learned from Enhanced Exams at 500 Banks—and What Bank Directors Should Do

On November 3, 2014, the Federal Financial Institutions Examination Council (FFIEC) released its observations summarizing results of a cybersecurity examination work program conducted by regulators at 500 randomly-chosen community banks. A major conclusion by the FFIEC as a result of this experiment is that the level of cybersecurity-related risk (after giving effect to existing security controls in place) “varies significantly across financial institutions.” That’s an indirect way of saying that regulators think some community banks really need to step up their game.

The FFIEC is obviously concerned that at some community banks the CEO and board members do not have enough awareness of (1) how much cybersecurity-related risk exists in the particular systems and services that the institution is using, and (2) whether the security controls in place at the institution are adequate to reduce that risk. Regulators expect senior management and the board to be directly responsible for controlling cybersecurity risk. This obviously cannot happen without asking the right questions about cybersecurity and analyzing enough information to understand clearly what level of risk the institution has, and how effective the institutions’ security controls may be.

The FFIEC’s document is another step in the regulators’ intensifying emphasis on cybersecurity. The FFIEC recommends two approaches that will help CEOs and directors to focus increased attention on cybersecurity risks:

First, the FFIEC lists 20 questions (each of which is discussed below) that CEOs and board members should ask themselves regarding cybersecurity. This is designed as a sort of diagnostic self-test. If CEOs and directors cannot answer these 20 questions, they may not have a strong enough understanding of the bank’s security risks and whether the mitigating controls that are in place are adequate.

Second, the FFIEC recommends that regulated financial institutions participate in the Financial Services Information Sharing and Analysis Center (FS-ISAC). This resource provides information about newly developing cybersecurity threats. The reason for learning about these current risks is so that the bank can promptly implement appropriate security controls to mitigate the developing risks. The problem with that suggestion, however, is that community banks may lack sufficient technical expertise internally to understand either (1) the specific security vulnerabilities that cyber attackers are targeting, or (2) the available security strategies that a bank could implement to mitigate those vulnerabilities.

As part of its service to client banks, BankOnIT remains constantly aware of newly developing security threats, and promptly applies appropriate security strategies to limit those risks. BankOnIT subscribes to FS-ISAC security feeds (mentioned above by the FFIEC), participates by invitation in confidential regulatory briefings on information security, and maintains current knowledge of industry-standard security practices for reducing a bank’s cybersecurity risks—so that a client bank will not have to bear the burden of wading through and resolving these sometimes highly-technical issues on its own.
The FFIEC has listed each of the following 20 bold-faced questions for CEOs and directors to ask themselves in order to evaluate whether they have sufficient awareness of their bank’s cybersecurity risks; what security controls are in place; and how much “net risk” remains (i.e., what level of risk is not eliminated even with those security controls in place). The discussion following the questions (“Suggested Action Steps” and “BankOnIT’s Solution”) are provided by BankOnIT, not the FFIEC.

I. CYBERSECURITY INHERENT RISK

1. What types of connections does my financial institution have?

   **Suggested Action Steps:**
   
   (a) A bank should prepare a list of all of the types of connections that exist, over which the bank’s data can flow. (If data can be transmitted over a particular technology path, data possibly also can be improperly accessed across that path if adequate security controls are not in place. As the FFIEC notes, “[E]ach connection represents a potential entry point for attacks . . .”) Bank technology systems have become so complex that a bank’s CEO and directors may be unaware of some of the data connections that exist, including electronic interconnections between the bank and its various service providers and vendors.

   (b) It would be helpful if the bank’s list of connections also included an explanation of how each connection is used, and/or why it is necessary. Reviewing the list might reveal some ways to improve security by reducing the number of connections.

   **BankOnIT’s Solution:**
   
   BankOnIT configures a bank’s network so that almost all connections are managed through BankOnIT. BankOnIT provides a network diagram for each client showing all of these connections, including VPN connections across the Internet (which are also documented and logged). This diagram is a useful visual aid to understand what exists.

   BankOnIT also performs assessments of internal vulnerabilities (annually) and assessments of external vulnerabilities (monthly) for client banks. Among other things, these assessments report on any perceived security weaknesses that exist with respect to the bank’s technology connections of all types that are within BankOnIT’s reach. For the CEO and directors, these vulnerability assessments serve as a status report on the configuration of the bank’s systems. BankOnIT’s main purpose for performing these assessments is diagnostic, to verify that the systems it manages are set up properly. But BankOnIT also turns the assessments into an “action list” that it then uses to take corrective action to limit or eliminate the identified vulnerabilities in reasonable ways.
2. **How are we managing these connections in light of the rapidly evolving threat and vulnerability landscape?**

**Suggested Action Steps:**

(a) **Someone acting on the bank’s behalf must regularly monitor “the rapidly evolving threat and vulnerability landscape”—which may include new viruses, newly discovered software vulnerabilities, and patterns of cyberattacks being launched against other banks.** It’s necessary for someone to keep track of newly-developing security threats, so that the bank will be adequately warned of those threats, and will know to apply available security strategies that can counter those new threats. Community banks are often not able to perform this function well on their own.

(b) **The CEO and directors themselves must have an active, ongoing role in this process.** The FFIEC wants a bank’s CEO and directors to ask themselves, “How are we managing these connections?” At most banks the directors may review a new banking system or new electronic product as it is first being approved and related connections are first set up. However, the FFIEC is asking for something more than a “once and done” decision-making process. The CEO and each director should have an ongoing, current knowledge of what data connections the bank has for its various systems and electronic banking products, and whether effective security controls continue to be applied to safeguard those specific connections against cyber attacks.

(c) **The CEO and directors need to be receiving up-to-date information about the current status of the bank’s systems—including connections.** “No news” flowing to the board about information security is not “good news.” On the contrary, “no news” may be a very good indicator that the bank’s level of attention to cybersecurity risks is deficient. The CEO and directors cannot just “assume” that the bank’s data connections are adequately protected, if no one is informing them about (1) newly developing security threats, (2) the security measures that would be necessary to counter those threats (applying new software patches, changing available security settings, using enhanced monitoring and reporting, etc.), and (3) whether the bank actually has those appropriate protections in place. **Information security is a constantly moving target—not a one-time fix.**

(d) **The security of each of the bank’s data connections must be evaluated separately.** There is no “one size fits all” security strategy for managing all of a bank’s data connections. Different types of connections have different purposes, and raise different issues. Some are more heavily used, and some transmit information that is much more sensitive. Some electronic banking systems are configured with very sophisticated security controls, but a bank may not be using the most secure settings available. Some connections have inherent weaknesses that need careful analysis for ways to increase protection.

(e) **Every data connection needs to be identified and analyzed.** It’s not enough to consider “most of them.” A cyber attacker will probe for any entry point into a bank’s systems until he finds the weakest information security link.
BankOnIT’s Solution:

BankOnIT regularly monitors the cyber security “threat and vulnerability landscape” on behalf of its client banks (see Question 9 for more details), and keeps a bank’s systems updated with industry-standard security strategies, patches, upgrades, etc.

When it first establishes services for a new client bank, BankOnIT configures the bank’s systems in ways that are more efficient, more secure and more reliable. On an ongoing basis BankOnIT performs vulnerability assessments (see Question 1 for more details) to analyze a bank’s data connections and other security aspects of a bank’s systems.

BankOnIT relies on its experience in working exclusively for banks, as well as multiple layers of security strategies, when it installs security controls to protect a bank’s data connections. (Some connections, such as for the bank’s core system, may be controlled by the vendor providing that particular service. As a result the bank should ask the vendor what security methods that vendor is using).

To make sure the board has adequate security information available, BankOnIT generates regular reports on the bank’s systems. (These reports are available through BankOnIT’s secure management console, in two versions: A technical format appropriate for examiners and auditors, and a non-technical format with graphs, suitable for presentation to the bank’s board.)

BankOnIT also provides CEO e-mail alerts, “white papers” and CEO newsletters (see Question 6), on topics that are specifically written for senior management but are also appropriate for reporting to the board, including emerging security threats, information on what security responses BankOnIT is providing, and commentary on recently issued regulatory guidance and other developments related to I.T.

3. Do we need all of our connections? Would reducing the types and frequency of connections improve our risk management?

Suggested Action Steps:

(a) Check for any bank connections that remain “open for access” although they may no longer be needed. (b) Consider reconfiguring the bank’s systems to reduce the total number of required connections. (c) Consider restricting the times that higher-risk connections are available for use.

Every separate connection that exists to connect the bank’s data to “something outside the firewall”—whether that outside connection may be from the public Internet, external networks, remote vendors, etc.—is an additional path over which a bank’s data might be accessed by cyber-attackers if adequate security controls are not in place.

Appropriate security controls can greatly reduce the risk that is created by allowing connections through the bank’s firewall. Still, no combination of controls can completely eliminate cyber risk. Even after industry-standard security controls are in place, CEOs and directors must recognize that every connection involves some continuing level of risk. (Ideally that risk can be mitigated to a low level.)
A bank’s CEO and directors should evaluate, for example, whether a particular type of connectivity that may not have much value to the bank should be allowed to continue to exist. (Does the benefit of each of the bank’s connections justify the risk?)

In some cases a connection involves considerable risk but still serves an important purpose. Internet connectivity is a good example: There’s no way to completely eliminate a bank’s risk from being connected to the Internet, except to disconnect the bank from the Internet—something that is not possible for a bank providing electronic banking services that customers expect. A degree of vulnerability will always exist, from being connected to the Internet. The next-best approach (ruling out “pulling the plug” on the Internet) is to apply a combination of security protections that can control Internet-related risk in all reasonable ways.

**BankOnIT’s Solution:**

As part of the service performed for client banks (see Question 1 for more details), BankOnIT examines a bank’s internal and external connections. In some cases, a bank may have a no-longer-needed “port” existing through the Internet firewall. (Originally this may have accessed the services of a former vendor, or a specific piece of equipment that the bank no longer uses. BankOnIT assists a bank by eliminating unused connections of this type, to reduce unnecessary risk.)

As part of the initial process of establishing services for a client bank, BankOnIT looks for ways to simplify a bank’s I.T. systems. Configuring systems to eliminate unnecessary complexity can almost always make systems operate better, and more reliably. Simplifying a bank’s technology systems may also reduce the number of data connections that are necessary, with no reduction in available services, but reduced cyber risk. Another way a bank usually can reduce its total connections, improve security and reduce the amount of due diligence required is by obtaining more of its outsourced services from a smaller number of vendors.

Regarding other vendors’ services, a bank should consider whether an infrequently-used but important connection that is “always on” could instead be turned off when not in use, or at least “time-restricted” for better security. As one example, some correspondent banks’ wire transfer programs let a local bank “time-restrict” wire-transfer authorizations, so that they can be approved only on banking days, or specific ranges of time each day.

Another way of “time-restricting” a connection is to consider not allowing an “always-on” connection for a vendor if maintenance on a bank’s systems is needed only infrequently. This can be accomplished by means of a secure web-support tool where a bank employee decides on each occasion whether to grant permission for the vendor to access the bank’s system to perform maintenance.

4. **How do we evaluate evolving cyber threats and vulnerabilities in our risk assessment process for the technologies we use and the products and services we offer?**

**Suggested Action Steps:**

(a) Community banks must remain familiar with changing cyber threats and vulnerabilities. More specifically (see Question 5), (b) a bank should understand how specific developing security threats may affect the particular technologies, products and services that the bank is using or offering.
But it’s often more than a community bank can do on its own, to understand the technical details of emerging cyber risks, and how or why the bank’s specific systems may be vulnerable. The regulators are aware that an “information gap” often exists in this area, but still they require banks to have this information and discuss it (see Question 6)—because without it, the CEO and directors cannot effectively “manage” the bank’s cyber risks.

(c) A bank is not permitted to completely hand off the issue of cyber risks to a vendor, without managing what is happening: The bank must continue to supervise and monitor the vendor’s activity. The bank’s CEO and directors are still required to have a process for (1) staying informed about cyber risks in general, and (2) keeping close enough tabs on a vendor’s activities to know how cyber risks in the bank’s systems are being managed.

**BankOnIT’s Solution:**

BankOnIT is experienced in evaluating evolving cyber threats and security vulnerabilities and applying available security strategies to counter those increased risks on behalf of a client bank. (For an explanation of how BankOnIT gathers information on evolving cyber threats and vulnerabilities, see Question 9. For more detail on how BankOnIT applies this information to improve risk management practices at a bank, see Question 10. Also see Question 11, for a discussion of reports that BankOnIT provides, which can be used to keep the board informed about cyber events and threats. Question 6 explains a process that can ensure ongoing and routine discussions by the board and senior management about cyber threats and vulnerabilities—as the regulators require.)

**5. How do our connections, products and services offered, and technologies used collectively affect our financial institution’s overall inherent cybersecurity risk?**

The FFIEC uses a new term, “cybersecurity inherent risk.” This is “the amount of risk posed by a financial institution’s activities and connections, notwithstanding risk-mitigating controls in place.” (It’s the overall level of “net risk” that remains for the bank, even after security controls are applied.) Cybersecurity inherent risk takes into account “the type, volume and complexity of operational considerations, such as connection types, products and services offered, and technologies used.”

**Suggested Action Steps:**

(1) CEOs and directors must first recognize there will always be some level of remaining “net risk” for the bank, if the bank chooses to engage in technology-related activities, products and services. Simply being connected to the Internet, having data connections, using technology systems, and offering electronic banking products or services, will automatically expose the bank to a certain amount of cyber risk. What is the bank doing to manage and mitigate this risk?

(2) Regulators expect a bank’s CEO and board to determine “how much” net cybersecurity risk the bank is facing, after giving effect to whatever security controls are in place. Of course, the overall level of remaining risk is the sum of the separate risks (after applying security controls) for each separate technology, or electronic product or service, which the bank is using or offering. The overall net cybersecurity risk is what the bank faces by continuing to operate in the way it is currently operating.

(3) A third step (implied, but required) is that the board will take whatever additional action is appropriate to further reduce net cybersecurity risk, if this risk is currently too high.
**BankOnIT's Solution:**

When BankOnIT initiates services for a client bank, it configures the bank's systems to provide multiple layers of security controls. Based on an initial “strategic review,” BankOnIT works to eliminate, or at least mitigate, security vulnerabilities that exist. The CEO and board of directors should recognize that some vulnerabilities can never be totally eliminated if the bank chooses to engage in the basic activity that introduces the risk. In the example previously given, if the bank is connected to the Internet—which is essential—that decision involves a certain inherent risk that can never be reduced to “zero,” short of disconnecting the bank from the Internet. Still, a variety of security controls can be applied to reduce risk in reasonable ways.

As new cyber threats and other security risks develop, BankOnIT continues to apply proven strategies at a client bank to counter those emerging risks.

BankOnIT helps to prepare I.T.-related policies for banks. (See Question 6 for more information.) These policies impose standards and guidelines covering, among other subjects, (1) how a bank's technology will be acquired and protected from risks, and (2) steps that the bank's officers, committee and board will carry out to provide appropriate monitoring and review of I.T.-related issues.

As part of an Information Security Policy that BankOnIT helps to provide, client banks prepare an Information Security Risk Assessment—an overview of risk, required by regulators, which presents in a summary format a bank's “net” risk (after security controls are in place) with respect to each of the bank's various major technology-based systems, activities, and products. This risk assessment is useful in helping the board to arrive at conclusions concerning the bank's overall net security risk.

As stated earlier, some banks have much more “cybersecurity-related risk” than others. In some cases there may be more than one reason why higher risk exists. Here are several examples of what might lead to higher cybersecurity-related risk at a bank: (a) Some banks are on the cutting edge in offering new electronic banking services—and have made a deliberate marketing-based decision to offer those activities in ways that can create a higher risk profile. (b) Some banks lack strong security controls, and may not understand how seriously a cyber attack could affect their operations. (c) Some banks also may be using one or more key vendors that have security-related deficiencies—lack of strong security controls, lack of experience working with banks, and/or insufficient familiarity with bank regulatory requirements. (d) Some banks may have written policies and procedures that say the right things, but the bank doesn’t follow them. As possible examples, training is not occurring; software patches are not being applied; known security vulnerabilities identified in exams and audits are not being addressed; committees are not meeting; vendor reports on the bank’s key systems are not being reviewed; and appropriate information-security-related issues are not being presented for review by management and the board.

Knowing why the bank has excessive risk is essential before senior management and the board can take appropriate steps to reduce that risk.
II. CYBERSECURITY PREPAREDNESS

a. Risk Management and Oversight

6. What is the process for ensuring ongoing and routine discussions by the board and senior management about cyber threats and vulnerabilities to our financial institution?

Suggested Action Steps:
A bank must have good procedures (1) that cause relevant cybersecurity information to be made available to the CEO and the board on a regular basis, and (2) that result in appropriate discussion and action by the board with respect to that information.

BankOnIT’s Solution:
BankOnIT helps a client bank to prepare information-security-related policies. These policies outline an internal process that causes important information-security-related issues and details to flow upward within the bank to the CEO and the board of directors. Here are some examples of steps required by the policies: An Information Technology Committee meets at least quarterly, vendor system reports are reviewed, written minutes are prepared, and all of the committee’s important actions and deliberations are in turn reported (both verbally and in writing) to senior management and the full board. Any serious information security events or issues are required to be reported promptly to the board. The board receives a comprehensive annual information security report. Annual vendor due diligence on key vendors is also summarized and presented to the board. The board adopts/readopts/revises on an annual basis an Information Technology Strategic Plan, an Information Security Policy (including an Information Security Risk Assessment), an Information Technology Systems Policy, and a Business Continuity Plan. Results of annual I.T. audits and of regulatory I.T. exams are also provided promptly to the board, and thereafter the board receives periodic status reports on the bank’s progress in dealing with any exception items.

BankOnIT also takes various steps to make sure that appropriate cybersecurity-related information is made available to client banks. BankOnIT provides e-mail alerts to bank CEOs concerning developing information security threats and current regulatory guidance or notices related to information security. BankOnIT prepares “white papers” (like this one) for distribution to CEOs, usually several times a year as developments occur. In addition, BankOnIT prepares CEO newsletters from time to time on information security topics.

With the reporting processes described above in place, “the process for ensuring ongoing and routine discussions by the board and senior management” is as simple as having the board review and discuss regulatory pronouncements, exam and audit information, pertinent news articles, and the various types of systems reports and general risk-related information that BankOnIT makes available—combined with similar information provided by the bank’s other “critical services” vendors.
7. How is accountability determined for managing cyber risks across our financial institution? Does this include management’s accountability for business decisions that may introduce new cyber risks?

**Suggested Action Steps:**

(1) A bank must establish a clear “chain of command” with respect to all information-security-related issues. The board itself must retain ultimate decision-making authority and oversight for all major information-security-related issues. Day-to-day information-security-related tasks should be assigned to a specific individual, who will be held accountable and must report regularly to a committee, senior management, and the board with respect to such matters as reviewing vendor reports, conducting vendor due diligence, coordinating with vendors, carrying out staff training, preparing revisions to policies, implementing regulatory guidance, resolving examiners’ or auditors’ exception items, and generally providing information on all relevant topics to a committee, senior management and the board.

(2) Historically, senior management has been held accountable for a bank’s financial performance (particularly with respect to loans). Making management accountable to the board for business decisions that introduce cyber risks should become another board priority. Establishing and enforcing an appropriate “risk culture” across many areas is important for a bank’s success. Examiners already view information security risk as bank’s third-highest risk, behind only lending risk and interest-rate risk.

**BankOnIT’s Solution:**

For client banks using BankOnIT-provided I.T. policies, an Information Security Officer is named as the person immediately responsible for all information-security-related issues. This person reports verbally and in writing to senior management and the I.T. Committee. In turn, a representative of the I.T. committee (usually the Information Security Officer) reports verbally and in writing to senior management and the board concerning that committee’s actions and recommendations. The Information Security Officer is also generally accountable to the bank’s C.E.O. for proper performance of job responsibilities.

For client banks, BankOnIT takes primary responsibility for identifying and implementing security strategies related to the bank’s network. (For the bank’s other “critical activities” vendors, a similar process may apply.) In all cases, however, the bank retains responsibility for overseeing what BankOnIT (or another vendor) does, both (1) by asking questions and receiving information, and (2) by reviewing vendor reports that are provided. Conclusions drawn, or exceptions noted, from this ongoing process of overview, interaction, and reporting should be summarized by the Information Security Officer to senior management and the committee, and in turn to the board.

Regulators expect a bank’s board to conduct an appropriate risk/benefit analysis before making a decision either to use an important new technology or to offer an important new electronic banking product.

Whenever a product, service, or system may introduce cyber risks, regulators would like to see documentation in the board minutes that the board (1) recognizes the potential risks, (2) is putting appropriate mitigating controls in place, and (3) understands what quantity of “net” risk remains even after security controls are in place.
With those factors understood, the board should document its “business decision” to accept the remaining risk, because it has determined that the potential benefit from that technology (or engaging in that service) outweighs the “net” risk that remains.

Ultimately, any decision about new products or services that could introduce new cyber risks for a bank should be made only by the CEO and/or the board. It may be wise for the CEO and the board to seek input about possible cyber risks, and appropriate mitigating controls, before making any major new product/new service decision. The Information Security Officer can gather documentation on potential providers and the security controls available from them. BankOnIT, because of its familiarity with multiple vendors, can provide information and advice when client banks are considering many types of technology changes.

Also, when a bank acquires any new technology or offers a new service that may involve cyber risks, it’s appropriate to consider adding a new line entry (or expanding an existing line entry) in the bank’s Information Security Risk Assessment, to list appropriate mitigating controls and the resulting “net” risk level.

8. What is the process for ensuring ongoing employee awareness and effective response to cyber risks?

Suggested Action Steps:

(1) Proper and frequent training of bank employees is essential to keep them alert to current security issues and to avoid information security mistakes and scams.

(2) Community banks’ employees generally have no ability to respond to the technical aspects of a cyber attack. However, employees should be trained in how the bank would manage an appropriate customer-facing response to a cyber attack in compliance with provisions of the bank’s Business Continuity Plan and/or Incident Response Plan. (The bank should determine that each “critical services” vendor is capable of managing for the bank the technical aspects of a cyber attack.)

BankOnIT’s Solution:

BankOnIT prepares and distributes Information Security E-Newsletters to client banks, monthly or bi-monthly. These newsletters provide current information, written on a non-technical level and suitable for employee training distribution to client banks. (Subjects covered include many of those listed below, as well as information and warnings about current security threats.)

Banks should emphasize a variety of topics in employee training throughout the year, to keep employees’ awareness of information security at a high level. (Apart from specific topics listed below, employees must also be trained annually on elements of the client bank’s Business Continuity Plan and the Information Security Policy.)

Some examples of appropriate topics for employee training (or “refresher” information) throughout the year include the following: (1) Passwords. A bank should place strong emphasis on enforcing password-based controls, including complex passwords that are longer and are changed frequently. Employees should use different passwords across different platforms, should avoid
obvious passwords, and should never write passwords down or reveal them to anyone else. (2) Unsecure/Secure E-mails. A bank should regularly emphasize to its employees that they should never include customer’s confidential information in ordinary e-mails, which are not secure. Forwarding internal bank e-mails outside the bank (such as to a personal mobile device or home computer that is not on the bank’s network) is also not secure. A secure e-mail system (which BankOn IT provides) should always be used when sending any type of confidential information outside of the bank’s internal secure network. (3) Pretext Calling and Social Engineering; Phishing. Employees should be trained annually on how to recognize and avoid responding to these security exploits. (4) Suspicious E-mails; Malicious Downloads. A bank should already have in place e-mail filtering (which intercepts most e-mails infected with a virus), web-content filtering, and an appropriate Employee Acceptable Use Policy (all of which BankOnIT provides). Beyond this, employees should be trained (a) not to open suspicious e-mails (which may contain a virus), (b) not to open links in e-mails received from unexpected sources (which may be a trick to induce the employee to download malicious software), (c) not to visit web sites that are not used in relation to bank business (which may be the entry point for a virus or malicious software), and (d) not to download any type of application to a bank-owned device (workstation, Smartphone, etc.) without permission (because this also may introduce a virus). (5) Regular Review of Vendor Reports. Not only to provide appropriate oversight of key vendors, but also to monitor for any security events that may require further action, a bank’s operations personnel should be trained to regularly review all vendor reports concerning activity or status of key systems. (As examples, firewall monitoring reports and e-mail filtering reports show how much undesirable incoming activity is being successfully blocked. Server maintenance reports and patch-management reports show whether the bank’s systems are being kept up to date, or instead may need some corrective action so the bank will be better able to repel information security attacks.) (6) Review of and Action on Vulnerability Assessments, I.T. Exam Reports, and I.T. Audit Reports. Operations personnel, senior management and the board should all be made aware of the need to follow up promptly on any information-security-related deficiencies noted in vulnerability assessments or exam or audit reports—so that the bank’s information-security defenses can be made stronger. (When vulnerability assessments are performed by BankOnIT, any weaknesses that are noted in a bank’s systems are automatically turned into an action list for BankOnIT to resolve. If a BankOnIT-client bank receives systems-related criticisms as the result of an I.T. exam or I.T. audit, BankOnIT works to help the bank eliminate those criticisms.)

(See Question 13 for an explanation of how BankOnIT would respond to a cyber attack on behalf of a client bank. Question 12 explains BankOnIT’s role in notifying regulators if such an event occurs.)

b. **Threat Intelligence and Collaboration**

9. **What is the process to gather and analyze threat and vulnerability information from multiple sources?**

**Suggested Action Steps:**
A bank cannot be prepared to meet emerging cyber threats and other security vulnerabilities, unless that bank has an adequate means of gathering information about (1) those threats and vulnerabilities, as well as (2) appropriate security measures to counter those risks. Most community banks cannot carry out this role for themselves—and must be sure they are hiring knowledgeable vendors who can assist them.
BankOnIT’s Solution:
As mentioned briefly above, BankOnIT subscribes to FS-ISAC security feeds (as the FFIEC recommends); participates by regulatory invitation in confidential briefings on information security; monitors and promptly evaluates for compliance action all bank regulatory warnings or guidance related to I.T.; remains updated on newly developed hardware and software products as they become available; and works to meet or exceed industry-standard security practices, including those specifically designed to defend against cyberattacks. Because BankOnIT works for so many banks, it can respond rapidly and proactively with respect to all of its client banks whenever it sees something at one bank that needs to be applied to other banks also—for example, a regulatory comment or apparent new emphasis, or a software issue that could cause problems.

BankOnIT monitors I.T. publications, business publications and general news articles with respect to I.T.-related issues. BankOnIT also maintains dialog with bankers and banking trade associations in multiple states.

BankOnIT sends e-mails and “white papers” to client-bank CEOs whenever a significant information-security development occurs that should concern banks—for example, new regulatory guidance, or more general I.T.-related news that could cause concern for bankers or bank customers.

BankOnIT provides security-related information to individual banks, case by case, either verbally or by e-mail, in response to bankers’ questions. On a daily basis, BankOnIT’s help-desk technicians provide advice and implementation concerning such matters as better mitigating controls and improved security settings and systems configurations.

BankOnIT also alerts client banks on critical information security issues specifically related to each bank (examples include items such as employee requests for more access than approved or failed log-in attempts from outside the network).

10. How do we leverage this information to improve risk management practices?

Suggested Action Steps:
A bank must have a vendor capable of implementing appropriate security measures promptly. Learning about emerging cyber threats and vulnerabilities is only the first step. A bank also must know (1) whether its own specific systems are susceptible to the problem, (2) what remedies (such as a newly-available software patch or enhanced system settings) may be available to reduce or eliminate the specific risks, and (3) how to implement those remedies—without potentially causing an unintended impact on other systems at the same time. It is difficult or impossible for a community bank to maintain this level of technical knowledge internally.

BankOnIT’s Solution:
BankOnIT uses all the information it is gathering from multiple sources—and the experience it has gained in working for many banks—to improve each client bank’s risk management practices, across the board. Whenever BankOnIT becomes aware of some type of improved security controls, or it internally develops an enhanced process, that knowledge can be leveraged to assist all client banks.
BankOnIT’s knowledge and expertise gives a client bank quick access to security controls and processes that respond to newly emerging threats. The bank does not have to go through an internal process of studying the problem, researching possible solutions, and waiting for a certain period of time before a qualified technician has time available to implement appropriate controls. With remote management software, BankOnIT can install software-based security controls promptly - without making a trip to the bank, and usually outside of banking hours to avoid disrupting operations.

11. What reports are provided to our board on cyber events and trends?

**Suggested Action Steps:**
At least several times a year, there is some important cyber-threat-related news or new regulatory guidance that the board should review promptly. A bank may want to consider adding a regularly recurring item such as “cyber events and trends” or “information security risks” to the board agenda each month. Listing this as a regular agenda item will be a reminder to ask the Information Security Officer and/or the CEO if a report will be prepared on this topic this month. In months when there is nothing to report, the board can skip over this agenda item by noting “no report” in the minutes.

**BankOnIT’s Solution:**
BankOnIT gives the bank a foundation on which information security issues can be reported to the board. BankOnIT sends broadcast e-mails and “white papers” to CEOs, explaining recent regulatory guidance, cyber events in the news, and how BankOnIT is protecting a client bank’s systems against specific types of threats. (See response to Question 9.) BankOnIT also provides regular written reports with respect to the status of bank systems that BankOnIT manages. The bank can supplement BankOnIT’s information with similar information provided by the bank’s other “critical activities” vendors. These various sources form a good basis for reports to the board concerning cyber events and trends.

12. Who is accountable for maintaining relationships with law enforcement?

**Suggested Action Steps:**
Before any incident has occurred, a bank should delegate to a specific officer the authority to communicate with law enforcement during and following an information-security-related event. Doing so can help the individual to plan what might be required, or to “role play” as part of a training event. Knowing who has this authority can help to avoid a case where an appropriate response to an actual event is delayed because (1) no one knows who has authority to take action, or (2) each person who might do so is focused on other priorities.

**BankOnIT’s Solution:**
BankOnIT helps client banks to prepare an Incident Response Plan (required by regulators). This plan covers two specific scenarios—where (1) a bank’s customers’ nonpublic personal information has been accessed (or may have been accessed) without authority, or (2) the bank is affected by an attack. In the Incident Response Plan provided by BankOnIT, a bank’s Information Security Officer is typically the person designated to contact law enforcement authorities. BankOnIT will assist law enforcement as required.
c. Cybersecurity Controls

13. What is the process for determining and implementing preventive, detective, and corrective controls on our financial institution’s network?

*Suggested Action Steps:*

Someone with appropriate knowledge of security threats and industry-standard practices for countering those threats must be placed in charge of “hands-on” management of security risks in the bank’s systems. This person must have authority to do what needs to be done (while reporting to and being supervised by the Information Security Officer and/or senior management). This person should have enough time available and capability to respond quickly to protect the bank’s systems or to respond to other I.T. problems.

(Caution: Security controls should be tested before they are applied. Most community banks do not have separate production and testing systems. As a result, installing software updates for a specific issue can cause an application or other inter-related systems to stop operating. Choosing a solution and properly implementing that solution are two separate issues to be considered.)

*BankOnIT’s Solution:*

BankOnIT chooses and implements technology-based security controls for client banks—not only to mitigate any generally known information security risks but also to defend against newly developing cybersecurity threats—as part of BankOnIT’s comprehensive solution, Bankers Private Cloud®.

BankOnIT also puts various strategies in place to detect attempted or ongoing attacks on a client bank’s systems. BankOnIT’s live 24/7/365 firewall monitoring can quickly detect malicious activity, allowing BankOnIT’s technicians to take action promptly to cut off the source of the attack.

When a bank’s vulnerability assessments, I.T. exams, or I.T. audit reports indicate that corrective controls may be needed with respect to network information security, BankOnIT reviews those exception items, compares them to any comments received in other examination and audit reports, and provides the bank appropriate documentation and technical assistance.

14. Does the process call for a review and update of controls when our financial institution changes its IT environment?

*Suggested Action Steps:*

Before installing new systems, hardware or software (including software updates), a bank should determine whether what is new will be compatible with what already exists. For example, will the proposed change cause something else to stop operating correctly? Or will it introduce new security risks that need to be considered and controlled?
**BankOnIT's Solution:**
The Information Technology Systems Policy provided to client banks by BankOnIT requires a bank to consider the compatibility of new hardware or software with existing systems. Risk assessments and vendor due diligence must be performed prior to acquisitions of new information technology systems or conversions, and vendor-provided access controls must be reviewed.

By working exclusively for banks, BankOnIT has gained a substantial depth of knowledge about the variety of applications that banks use. BankOnIT puts that knowledge to work for all client banks. By contrast, when a bank uses a local I.T. firm or I.T. person who works for only one or a handful of banks, each using varying applications, the local bank is operating in a “silo,” and must independently resolve issues and address security issues without the benefit of knowledge gained at other institutions. This can lead to delays in problem resolution, less reliability and greater cost.

15. **What is our financial institution's process for classifying data and determining appropriate controls based on risk?**

**Suggested Action Steps:**
A bank should provide adequate security for its data; but not all data is equally sensitive. Questions such as what combination of security controls a bank should use for certain data, whether certain data requires higher security and more limited access rights, or whether certain data should be encrypted, can have different answers depending on what the data consists of. (Unless a bank first understands what data is being stored and how sensitive it may be, it’s normally impossible to conclude whether the security controls protecting that data are adequate. For example, a database containing nothing but mailing addresses may be less important; but it would be disastrous if someone gained unauthorized access to a highly-confidential list containing many of the following categories—customer name, birth date, Social Security number, account number, Internet username and password, and deposit balance.)

**BankOnIT's Solution:**
With respect to bank data that is hosted or backed up at BankOnIT’s secure data center, BankOnIT has a simple solution for this problem: BankOnIT treats all of a bank’s data as if it is sensitive, non-public personal information. BankOnIT uses multiple types of physical, logical and policy-based controls to protect the security of data. (These controls are reviewed annually by independent auditors, with the audit report provided to client banks.)

(If other “critical services” vendors, such as a core processor, an imaging provider, or a mortgage loan software company, provide either off-site (remote) hosting of the bank’s data, or off-site backups of that data, the FFIEC’s question about “what kinds of data does the bank have and how is it protected” should extend to the operations of those third-party vendors as well.)

Even if all of a bank’s data is hosted offsite (for example, by BankOnIT, a core vendor, etc.), it’s still relevant to consider whether the level and combination of security controls in place at the bank is appropriate to protect against unauthorized access to sensitive data. This analysis includes questions that may be more “close to home” for most banks: Are screen-savers in place on desktops, timing out after a certain period of inactivity? Are employees required to use complex (and long) passwords and change them frequently?
Does an individual use a different password to access a system with more restricted access rights (not the same password as for the network)? Is access to all bank systems strictly limited on a “need to know” basis, determined by job responsibilities? When an employee’s job description changes, or a person leaves employment or is gone from the bank for an extended time, does someone promptly delete that person’s no-longer-necessary access rights for key systems?

BankOnIT assists banks in developing an Information Technology Systems Policy that follows the general guidelines of the FFIEC’s I.T. examination questionnaire. This policy imposes on the bank numerous procedure-based information security controls that examiners and auditors expect a bank to have. Having such provisions in a bank’s policies can help to smooth an exam or audit, but they are also even more important for their primary purpose—protecting the bank.

Not only during BankOnIT’s process of setting up a new client bank’s systems, but also on an on-going basis, BankOnIT provides answers for a client bank’s questions. BankOnIT is available to participate in strategic planning sessions with the bank’s board, and can give unbiased recommendations with respect to any proposed major changes in a bank’s systems.

16. **What is our process for ensuring that risks identified through our detective controls are remediated?**

**Suggested Action Steps:**

*Every bank must set up a system whereby someone is responsible for promptly taking action to address security risks and vulnerabilities as they are diagnosed or identified by various methods.* (Security is not being managed well if the bank has a list of what should be corrected, but it ignores the list. In information security, the longer a weakness in the bank’s systems goes uncorrected, the greater is the risk that someone could exploit that weakness to gain unauthorized access to information. Particularly when multiple “repeat issues” are listed by examiners or auditors that have not been corrected or responded to since the previous exam or audit, those reviewers may start to lose confidence in whether the bank’s CEO and board are strongly committed to managing and controlling the bank’s information security risks.)

Vulnerability assessments (discussed in Question 1) are one means of identifying risks and vulnerabilities that a bank needs to remediate if practical. System error reports are another source. Virus scans and firewall monitoring also may provide valuable information that should be acted on. The exception items and recommendations in an I.T. audit report, as well as an I.T. exam’s exceptions, may also be recognized as specific security weaknesses in a bank’s systems.

Sometimes a bank’s slowness in resolving risk issues may result from either a lack of expertise (an I.T. provider who lacks experience in carrying out necessary corrective steps) or a lack of budget (for example, the bank may be paying for I.T. services by the hour, and not willing to spend what it would take to accomplish everything that needs remediation). Unfortunately, neither of these restraints will impress regulators who want banks to reduce their security risks.

**BankOnIT’s Solution:**

BankOnIT takes responsibility for helping client banks to remediate risks that are identified through detective controls.
One example of detective controls in place (see response to question 13) is BankOnIT’s live 24/7/365 firewall monitoring. BankOnIT continuously monitors and manages the bank’s firewall to protect the bank’s network, including logging, analyzing and addressing any high-risk and critical events. With 24-hour staffing, BankOnIT many times is able not only to detect but also to resolve issues in the middle of the night or over the weekend, before those issues can even start to have an impact on the bank’s business-hours operations. Community banks are not staffed on a 24-hour basis, and even if the bank has internal I.T. personnel, a similarly prompt response by them would usually not be possible.

Another type of detective control provided by BankOnIT is vulnerability testing: BankOnIT performs internal vulnerability testing (annually) and external vulnerability testing (monthly) for client banks. BankOnIT’s main purpose in performing these tests is diagnostic—to verify the condition of systems that BankOnIT is managing for the bank. If vulnerabilities are identified by this testing, BankOnIT promptly works to eliminate, or at least to reduce as much as practical, the vulnerabilities that are identified. (Results of all vulnerability testing will be made available to client banks, which then can monitor whether remediation of those vulnerabilities is occurring.)

I.T. exam reports and I.T. audit reports can also be thought of as detective controls, to the extent that they may identify vulnerabilities that a bank needs to remediate. BankOnIT regularly helps banks with responses to exception items listed in an I.T. exam or audit.

**d. External Dependency Management**

17. How is our financial institution connecting to third parties and ensuring they are managing their cybersecurity controls?

**Suggested Action Steps:**

(1) A bank should prepare a list of all third-party vendors that are connected in any way to the bank’s data. (These are vendors that the bank needs to monitor carefully.) Included on this list is BankOnIT, as an I.T. support firm. This category also includes a core provider that either remotely hosts or remotely connects to the core system at the bank. A correspondent bank through which the bank electronically originates wire transfers and/or ACH payments is a similar case. Also, the bank’s ATM/debit transaction processor should be listed because of online access to the bank’s deposit information. Still more examples may include a bank’s telephone banking, Internet banking, mobile banking or merchant capture systems vendors. Electronic clearing of checks is technically another example of connectivity involving customer financial information. Beyond that, some banks may also be using a remotely-accessed imaging system or remotely-accessed mortgage origination program, either of which would fall in the same category if customer information is stored offsite or backed up offsite by those systems.

(2) The bank must determine how strong are the cybersecurity controls used by these third-party vendors who have access to important categories of bank data. When a bank “outsources” important portions of its necessary services to “critical activities” vendors, it is not enough to determine whether the bank’s own internal cybersecurity controls are adequate: In addition, the bank must determine whether the cybersecurity controls used by its key outsourced vendors are also adequate. (Outsourcing to a vendor cannot eliminate a bank’s responsibility to make sure
that cyber risks are adequately controlled. The bank is responsible for the fact that its data is inadequately protected, and that includes when the chosen vendor’s own cyber risk controls are inadequate. Using a vendor with inadequate risk controls is the same as the bank not establishing adequate risk controls.)

**BankOnIT’s Solution:**
BankOnIT provides extensive “due diligence” information to client banks. Importantly, BankOnIT receives annual “Technology Service Provider” examinations by the FFIEC (a copy of exam results is available from a client bank’s primary federal regulator), as well as annual SSAE 16 (Service Organization Control) audits by an independent CPA firm. (BankOnIT provides these reports to client banks). Both the FFIEC’s exams and the SSAE 16 audits involve an extensive review of BankOnIT’s security controls. Reviewing the exam results and auditor’s conclusions can provide important assurance to client banks concerning the status of BankOnIT’s internal controls.

With respect to each additional “critical services” vendor that the bank uses, it is the bank’s responsibility to gather similar information that will document or provide appropriate assurances that the particular vendor’s cybersecurity controls are strong. BankOnIT strongly recommends that a bank use only those key vendors that are obtaining exams from banking regulators as well as annual SSAE 16 audits, because for them the levels of review by examiners and auditors with technical expertise is likely to be much more comprehensive than any “due diligence” that a bank could perform entirely on its own on the adequacy of a non-regulated vendor’s security controls. Without access to regulatory exam results and SSAE 16 audit reports on a vendor, a bank must conduct a more detailed review of a vendor’s available written materials, and continue asking questions that are not answered by those materials, to attempt to reach a well-supported conclusion (if true) that each key vendor with access to the bank’s data is using appropriate cybersecurity controls in its own operations.

18. **What are our third parties’ responsibilities during a cyber attack? How are these outlined in incident response plans?**

**Suggested Action Steps:**
For each “critical activities” vendor that has access to the bank’s data, the bank should ask about the details of the vendor’s Incident Response Plan. Vendors familiar with banking compliance should already have this information available. A vendor that lacks this information may not have done adequate planning for a cyber attack.

“Critical services” vendors should already have strong cybersecurity in place. Regulators expect those vendors to plan for how they would respond if a cyber attack is successful—in other words, if certain customer information related to the bank is actually accessed (or may have been accessed) by the cyber attackers. Here are some key questions the bank should ask concerning what the vendor will do in that scenario: (1) Does the vendor agree to notify the bank of that incident? (2) Will the vendor assist by providing details the bank needs to contact its customers? (3) Who will be responsible (the vendor or the bank) for notifying law enforcement and regulators?

**BankOnIT’s Solution:**
(See Question 19 for BankOnIT’s response to both this question and Question 19.)
**e. Cyber Incident Management and Resilience**

19. *In the event of a cyber attack, how will our financial institution respond internally and with customers, third parties, regulators, and law enforcement?*

**Suggested Action Steps:**

(1) Each bank is required by regulators to have an Incident Response Plan, which should be broad enough to cover any known or suspected security breach with respect to customer information. (The Incident Response Plan will apply to a cyber attack or any other incident in which authorized access to customer information occurs by whatever means.)

(2) If a specific vendor’s services are involved with a cyber attack or other security breach, the bank’s own Incident Response Plan, taken together with that vendor’s Incident Response Plan, should provide a clear roadmap for what to do, who to contact, and who has responsibility for which steps.

**BankOnIT’s Solution:**

For client banks, BankOnIT helps to prepare an Information Security Policy, including an Incident Response Plan. BankOnIT also has an Incident Response Plan for its own operations.

If a cyber attack should occur with respect to a client bank, BankOnIT will handle the technical aspects of responding to a cyber attack. (BankOnIT provides 24/7/365 “live staffed” firewall monitoring, detecting and mitigating attacks in real time).

Using the FFIEC’s required assumption that a cyber attack would be successful in accessing some of a bank’s customer data, here is how the relevant response tasks would be divided between BankOnIT and the Bank:

(1) Because the bank’s customers will be unfamiliar with BankOnIT, any “messaging” that needs to be provided to affected bank customers should come from the bank. (BankOnIT assists the bank in developing appropriate messaging, and in determining which customers may have been affected.)

(2) BankOnIT, along with the bank, will advise the regulators of the incident, providing any necessary technical information that the regulators may need or request.

(3) As appropriate in the circumstances, BankOnIT will assist the bank in contacting law enforcement authorities, including any technical information about the source and details of the attack, as required.

*Important:* A bank must understand how the same incident-response process will work with each of its other “critical services” vendors. (The answers may be somewhat different when a different vendor—for example, the core vendor—is the target of the cyber attack.)
20. How are cyber incident scenarios incorporated in our financial institution’s business continuity and disaster recovery plans? Have these plans been tested?

Suggested Action Steps:

(1) In recent examinations and I.T. audits, the examiners and auditors have been requesting that banks develop a written plan for responding to a DDoS attack on the bank’s website. (A DDoS attack is one type of cyber attack, usually designed to “jam” a bank’s website so that customers are unable to use it. By itself, a DDoS attack does not put customer information at risk.)

(2) In this Question 20 the FFIEC goes farther, suggesting that banks should plan for a “cyber incident” as another type of “disaster recovery” or “business continuity” event. (Requesting this treatment asks a bank to assume that the “cyber incident” is successful: In other words, banks should consider what they would do in a scenario where some of their customers’ information has actually been accessed by a cyber attack, and/or the bank’s systems (or key vendors’ systems) have been compromised/disabled by the attack.)

BankOnIT’s Solution:

BankOnIT helps client banks to prepare an Information Security Policy, including an Incident Response Plan. This Incident Response Plan is written to cover a wide variety of incidents, including DDoS attacks.

BankOnIT also helps client banks to prepare a Business Continuity Plan, which names a Business Continuity Coordinator, a committee, response teams, and designated individual officers who are tasked with specific responsibilities if a business continuity event occurs. Some of the specifically designated tasks under the Plan include handling public announcements and communications, re-establishing connectivity, and contacting the regulators. The Business Continuity Plan requires the bank to carry out testing and employee training annually.
One example of detective controls in place (see response to question 13) is BankOnIT's live 24/7/365 firewall monitoring. BankOnIT continuously monitors and manages the bank's firewall to protect the bank's network, including logging, analyzing and addressing any high-risk and critical events. With 24-hour staffing, BankOnIT many times is able not only to detect but also to resolve issues in the middle of the night or over the weekend, before those issues can even start to have an impact on the bank's business-hours operations. Community banks are not staffed on a 24-hour basis, and even if the bank has internal I.T. personnel, a similarly prompt response by them would usually not be possible.

Another type of detective control provided by BankOnIT is vulnerability testing: BankOnIT performs internal vulnerability testing (annually) and external vulnerability testing (monthly) for client banks. BankOnIT's main purpose in performing these tests is diagnostic—to verify the condition of systems that BankOnIT is managing for the bank. If vulnerabilities are identified by this testing, BankOnIT promptly works to eliminate, or at least to reduce as much as practical, the vulnerabilities that are identified. (Results of all vulnerability testing will be made available to client banks, which then can monitor whether remediation of those vulnerabilities is occurring.)

I.T. exam reports and I.T. audit reports can also be thought of as detective controls, to the extent that they may identify vulnerabilities that a bank needs to remediate. BankOnIT regularly helps banks with responses to exception items listed in an I.T. exam or audit.

d. External Dependency Management

17. How is our financial institution connecting to third parties and ensuring they are managing their cybersecurity controls?

Suggested Action Steps:

(1) A bank should prepare a list of all third-party vendors that are connected in any way to the bank's data. (These are vendors that the bank needs to monitor carefully.) Included on this list is BankOnIT, as an I.T. support firm. This category also includes a core provider that either remotely hosts or remotely connects to the core system at the bank. A correspondent bank through which the bank electronically originates wire transfers and/or ACH payments is a similar case. Also, the bank's ATM/debit transaction processor should be listed because of online access to the bank's deposit information. Still more examples may include a bank's telephone banking, Internet banking, mobile banking or merchant capture systems vendors. Electronic clearing of checks is technically another example of connectivity involving customer financial information. Beyond that, some banks may also be using a remotely-accessed imaging system or remotely-accessed mortgage origination program, either of which would fall in the same category if customer information is stored offsite or backed up offsite by those systems.

(2) The bank must determine how strong are the cybersecurity controls used by these third-party vendors who have access to important categories of bank data. When a bank "outsources" important portions of its necessary services to "critical activities" vendors, it is not enough to determine whether the bank's own internal cybersecurity controls are adequate: In addition, the bank must determine whether the cybersecurity controls used by its key outsourced vendors are also adequate. (Outsourcing to a vendor cannot eliminate a bank's responsibility to make sure About the Author:

Charles Cheatham joined BankOnIT in 2009 as Senior Vice President and General Counsel. He has over 30 years of experience providing legal services and advice to bankers, including bank acquisitions, contracts, compliance, legislation, teaching and extensive writing about banking law developments.

Prior to joining BankOnIT he served for 12 years as Vice President and General Counsel of the Oklahoma Bankers Association and was previously a partner at McAfee & Taft, the largest law firm in Oklahoma.

Charles is a graduate of Oklahoma State University and Harvard Law School.

About BankOnIT:

BankOnIT is the exclusive developer and provider of the Bankers Private Cloud®, a unique cloud-based I.T. solution for community banks that improves efficiency, reliability, and information security while minimizing a bank’s risk – including regulatory and strategic risks – that are present in today's rapidly changing technology environment.

References