CSBS
SINCE 1902
CONFERENCE OF STATE BANK SUPERVISORS

CYBERSECURITY 101

A Resource Guide for **BANK EXECUTIVES**

Executive Leadership of Cybersecurity

CEO LETTER

I am proud to present to you the CSBS Executive Leadership of Cybersecurity Resource Guide.

The number of cyber-attacks directed at financial institutions of all sizes is growing. Addressing this new threat requires a concerted effort by community bank CEOs.

This is why the Conference of State Bank Supervisors, on behalf of state regulators, launched the Executive Leadership of Cybersecurity initiative (ELOC). The ELOC initiative is designed to engage bank executives and provide you the tools to address cybersecurity threats.

The information provided within this guide is tailored to furnish CEOs with the necessary tools to better understand the threats your institution faces and how to prepare for them. It also provides questions to ask your staff to ensure they are proactive in identifying and addressing cybersecurity risks.

Thank you for taking the initiative to make your bank, your customers, and your community safer while online. Your leadership, determination, and willingness to adapt are instrumental to maintaining a robust, secure financial system.

John W. Ryan
President & CEO, Conference of State Bank Supervisors

TABLE OF CONTENTS

Introduction 2

Identify 3

Protect 9

Detect 15

Cyber Threats 18

8 Mobile Banking Recommendations 20

Respond 22

Recover 27

Glossary 31

Sources 35

THE PERSISTENT THREAT OF INTERNET ATTACKS IS A SOCIETAL ISSUE FACING ALL INDUSTRIES, ESPECIALLY THE FINANCIAL SERVICES INDUSTRY. ONCE LARGELY CONSIDERED AN IT PROBLEM, THE RISE IN FREQUENCY AND SOPHISTICATION OF CYBER-ATTACKS NOW REQUIRES A SHIFT IN THINKING ON THE PART OF BANK CEOS THAT MANAGEMENT OF A BANK'S CYBERSECURITY RISK IS NOT SIMPLY AN IT ISSUE, BUT A CEO AND BOARD OF DIRECTORS ISSUE.

CYBERSECURITY:

The ability to **protect or defend** the use of cyberspace **from cyber-attacks.**

(National Institute of Standards and Technology, NIST)

INTRODUCTION

Cybersecurity experts expect the trend toward increasingly sophisticated cyber-attacks to continue in the near future. And the financial services industry, a vital component of the nation's critical infrastructure, remains a prime target for cyber criminals.

Cyber risks, like reputational and financial risks, have the ability to affect a bank's bottom line. It can be costly, compromising to customer confidence, and, in some cases, the bank could be held legally responsible. Beyond the impact to an individual bank, cyber risks have far-reaching economic consequences. Due to the inherent interconnectedness of the Internet, a security breach at a few financial institutions can pose a significant threat to market confidence and the nation's financial stability.

Symantec's 2014 Internet Security Threat Report revealed that a total of **253 data breaches** took place in 2013. This is an **increase of 62%** from 2012.

This reinforces the notion that safeguarding against cybersecurity threats is not a problem that can be addressed by any one bank. To adequately deal with the persistent threat of cyber-attacks, financial institutions and bank regulators must come together, collaborate, identify potential weaknesses, and share industry standards and best practices.

The goal of this document is to provide you, the bank CEO, with a non-technical, easy-to-read resource on cybersecurity that you may use as a guide to mitigate cybersecurity risks at your bank. This resource guide puts in one document industry recognized standards for cybersecurity, best practices currently used within the financial services industry, and an organizational approach used by the National Institute of Standards and Technology (NIST). While this resource guide is tailored for the community bank CEO and executive staff, all bank CEOs can benefit from this guide regardless of a bank's **cybersecurity inherent risk**.

While this resource guide does not guarantee protection against cybersecurity threats, it attempts to identify various resources—including people, processes, tools and technologies—that financial institutions can use to reduce the potential of a possible cyber-attack.

Cybersecurity 101 is organized according to the five core cybersecurity functions of the **NIST's Cybersecurity Framework**. These five functions provide organization and structure to the help your bank navigate its way to better protection against cyber threats. The five core functions of cybersecurity include:

01
IDENTIFY internal and external cyber risks.

02
PROTECT organizational systems, assets, and data.

03
DETECT system intrusions, data breaches, and unauthorized access.

04
Respond to a potential cybersecurity event.

05
RECOVER from a cybersecurity event by restoring normal operations and services.

IDENTIFY

CEO QUESTIONS

Questions bank CEOs should ask:

1. Does my institution fully understand what information it manages, where the information is stored, how sensitive is the information, and who has access to it?
2. What are my institution's "crown jewels" or key business assets? Do I have adequate protection for them?
3. What types of connections does my financial institution have (VPNs, wireless, LAN, etc.) and how are we managing these connections?
4. How is staff at my institution identifying risks, and providing me with accurate and timely information about those risks?
5. What is our ability to mitigate those risks?
6. How is my institution connecting to third parties and ensuring they are managing cybersecurity controls?

IDENTIFY

The first core cybersecurity function is to identify your bank's cybersecurity risk, which is the amount of risk posed by a financial institution's activities, connections, and operational procedures. A **risk** is the potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability.

To identify these risks, your financial institution should have a risk assessment, or a process for identifying threats to information or information systems, in order to determine the likelihood of the occurrence of the threat and to identify system vulnerabilities. A risk assessment should include the classification of critical information assets, identifying threats and vulnerabilities, measuring risk, and communicating risk.

Risk Assessment

1. Classification of Information
2. Identify Threats and Vulnerabilities
3. Measure Risk
4. Communicate Risk

Classification of Information

Before you can adequately assess risk to your bank, you must first identify what your bank's "crown jewels" are, where they are located, and how they are being protected. **Crown Jewels** are critical information assets that are regarded as highly sensitive, essential pieces of information to the organization.

"Crown jewels" could be people (e.g., employees or customers), property (both tangible and intangible), or information (e.g., databases, software code, critical company records).

After the "crown jewels" have been identified, all information assets should be classified based on a defined category of sensitivity. This can be carried out by an individual or a team. Classifications could include such categories as:

- **Confidential**—having a *severe impact* to the financial institution, its critical functions, business partners, or customers if lost, damaged, or if disclosure is unauthorized;
- **Internal Use Only**—having *minimal to limited impact* to the financial institution, its critical functions, business partners, or customers if lost, damaged, or if disclosure is unauthorized;
- **Restricted**—having *limited impact* to the financial institution, its critical functions, business partners, or customers if lost, damaged, or if disclosure is unauthorized; and
- **Public Information**—having *minimal to no impact* to the financial institution, its critical functions, business partners, or customers if lost, damaged, or if disclosure is unauthorized.

Your bank's critical information assets, or "crown jewels," should have the highest security classification level. The classification of your crown jewels and all other information should be included on the information itself and on a central list, often called a "key asset register" or a "crown jewels register." The classification of assets should be conducted periodically as asset classification may change based on business needs. Additionally, documented policies and procedures regarding the classification of documents should be in place so that all employees are aware and educated about them.

More information on classifying information assets is available from the SANS Institute InfoSec Reading Room at http://www.sans.org/reading-room/whitepapers/auditing/conducting-electronic-information-risk-assessment-gramm-leach-bliley-act-compliance-1053. The New York State Office of Cyber Security and Critical Infrastructure Coordination also has a resource at http://www.dhses.ny.gov/ocs/awareness-training-events/documents/InfoClassTrainingPresentation.pdf.

This same individual or team should be responsible for periodically assessing your bank's information assets and managing and reporting the risk.

Identify Threats and Vulnerabilities

In addition to classifying the bank's information assets, the individual or team should also identify potential threats and vulnerabilities to the financial institution's information assets.

A **threat** is a force, organization, or person that seeks to exploit a vulnerability to obtain, compromise, or destroy an information asset. A **vulnerability** is a weakness in a system or program that can be exploited by threats to gain unauthorized access to an information asset.

Identifying threats and vulnerabilities to your bank is critical. At any given time your bank could be exposed to several different types of information security threats. These threats include:

- *Natural disasters*, such as floods and fires;
- *Internal threats*, like malicious or unaware employees;
- *Physical threats* by a potential intruder; and
- *Internet threats*, such as hackers.

Consider what threats your bank is exposed to and what vulnerabilities may exist surrounding these threats. For example, an inherent threat that comes with using computers, laptops, or USB devices is the unintentional loss of data via identity theft or unsecure data. The vulnerability is the potential gaps that may exist in securing data on these devices such as an employee forgetting to secure his or her laptop, or a manager failing to encrypt sensitive data on the USB drive.

To identify potential cybersecurity threats, your financial institution may use internal resources, such as audit reports and fraud detection tools; or external resources, such as information sharing networks like the **Financial Services—Information Sharing and Analysis Center (FS-ISAC)**. In November 2014, the **Federal Financial Institutions Examination Council (FFIEC)** issued a statement recommending that financial institutions of all sizes participate in the FS-ISAC as part of their process to identify, respond to, and mitigate cybersecurity threats and vulnerabilities. Additionally, two publicly available reports that can provide current threat intelligence are Verizon's *Data Breach Investigations Report*, available at http://www.verizonenterprise.com/DBIR/, and Symantec's *Internet Security Threat Report*, available at http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf. Both reports are updated annually.

In identifying a potential vulnerability in infrastructure, systems, or applications, it is common to use "off the shelf" tools such as a vulnerability scanner or analyzer that can probe for the vulnerability using well-known network protocols and methods. These tools can also test the vulnerability to determine if it was in fact exploitable. Accurately assessing threats and identifying vulnerabilities is critical to understanding the risk to assets.

Measuring Risk

To measure your bank's level of risk, first develop a method for measuring risk. One approach is shown in figure 1 taken from the "Risk Management Non-Technical Guide" provided by the **Multi-State Information Sharing & Analysis Center (MS-IAC)**. Information assets are given a value of high, medium, or low. The risk level of those information assets is also given a rating of high, medium, or low. The final level of risk depends on actions taken by the bank. For example, if backups are done and secured, the loss of an electronic file may be a low risk.

FS-ISAC
for Community Banks

FS-ISAC offers a basic membership for community banks with less than $1 billion in assets which includes a number of "must-have" services shown below. To receive only the most critical public alerts, the smallest community-based institutions may elect to register as a Critical Notification Only Participant (CNOP). This service is offered free-of-charge but provides notification of ONLY urgent and crisis alerts that are public. Learn more at https://www.fsisac.com/join.

Figure 1. Measuring Cybersecurity Risk

Source: MS-ISAC

Information Asset	**Value** (High/Low/Medium)	**Risk Level** (High/Low/Medium)	**Notes** (Explain Major Risks and/or Costs)
Board Minutes	High	Low	Expectation is these are highly protected
Personnel Records	High	High (Identity Theft)	Have a high value to the organization for reporting, retiring Payroll, etc.

Communicating Risk

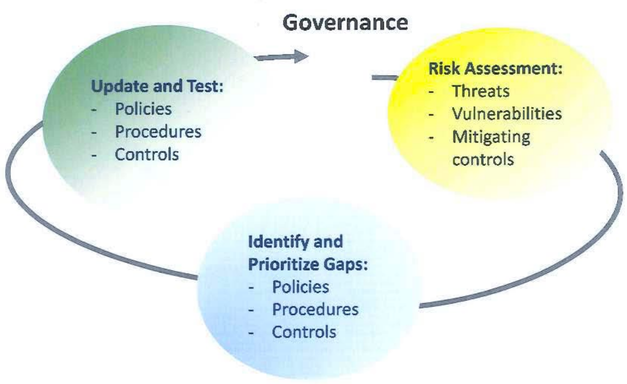
It is vital to have a process that informs senior management and the board of directors about cyber risks to your bank, how your bank currently manages them, how to mitigate those risks, and who is accountable for doing so. Once your financial institution has conducted a risk assessment and made decisions about how to mitigate those risks, reviews should be conducted at least annually.

Cyber Risk Management Process

The risk assessment is one element of a larger cyber risk management process that each bank should have in place. Bank CEOs should strive to create and implement an effective and resilient risk–management process to enable proper oversight and to ensure that you are effectively managing cybersecurity risks. Key elements of a risk–management (or cyber-incident management) process should include the initial assessment of new threats; identifying and prioritizing gaps in current policies, procedures, and controls; and updating and testing policies, procedures, and controls as necessary. More information on the risk-management process is available in the FFIEC's Executive Leadership of Cybersecurity webinar at https://www.brainshark.com/csbs/vu?pi=zGBzRS8LMz3pQMz0&intk=905196563.

Figure 2. Cyber Risk Management Model

Source: FFIEC



Inventory Authorized and Unauthorized Devices and Software

It is important to identify and actively manage all hardware devices on your network, including servers, workstations, laptops, and remote devices, so that only authorized devices are given access. Attackers, who may be located anywhere in the world, are continuously scanning the Internet address space of target organizations, waiting to identify unprotected and vulnerable systems in order to infiltrate the system and eventually gain unauthorized access to information.

Just as with hardware, it is equally important to actively manage all software on your network so that only authorized software is installed and unauthorized or unmanaged software is prevented from being installed or executed. Attackers continuously scan target organizations looking for vulnerable versions of software that can be remotely exploited.

Bank CEOs should ensure processes are in place to maintain a current and accurate view of all of their financial institution's assets, keeping in mind that doing so is an ongoing process that requires regular, consistent monitoring.

TOP 20 CRITICAL SECURITY CONTROLS

Inventory of Authorized and Unauthorized Devices

#1: Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

#2: Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

THE COUNCIL ON CYBERSECURITY

Each year the **Council on Cybersecurity**, located in the Washington, D.C. area, releases its *Top 20 Critical Security Controls*. These controls are meant to establish priority of action for organizations actively managing cybersecurity risks and to keep knowledge and technology current in the face of rapidly evolving cyber threats. The *Top 20 Critical Security Controls* is a reference set of recommendations to address risks to company data and systems. The Critical Security Controls will be referenced throughout this guide according to the core cybersecurity functions.

More information on the Council on Cybersecurity and the Top 20 Critical Security Controls is available at www.counciloncybersecurity.org

PROTECT

CYBERSECURITY 101

PROTECT

Once you have identified your bank's threats, vulnerabilities, and risks, the next core cybersecurity function is to ensure your financial institution has the appropriate safeguards or controls in place to mitigate the various types of threats to your bank. This is vital as your bank's protection measures are the "front lines" of defense in securing your information and crown jewels. These protection measures work to limit or contain the impact of a cybersecurity event or incident.

STAFF TRAINING

Cyber hygiene:
Cyber hygiene refers to steps computer users take to protect and maintain systems and devices.

Investing in time and resources to secure your network must include the human element—staff awareness and training. Too many organizations focus on the technology side of cybersecurity and forget the human element. Your staff plays a critical role in protecting your bank from Internet threats. As such, your staff can either be the weakest link in your bank's cybersecurity program or your greatest protection measure.

The practice of "safe" **cyber hygiene** can no longer be the responsibility of solely the IT department. Bank CEOs should put in place training to educate, motivate, and incentivize all employees to be vigilant and in a constant state of preparedness when it comes to cybersecurity. Your staff members need to understand the value of protecting customer and colleague information and their role in keeping sensitive data safe. Staff should also have a basic grounding in other cybersecurity risks and how to make good judgments online. Page 11 of this guide highlights resources for raising awareness and providing training for employees on cybersecurity.

Customer Authentication

Financial institutions should develop and implement security measures to reliably authenticate customers accessing financial services via a bank's website. The Federal Financial Institutions Examinations Council (FFIEC) issued guidance in 2005 that highlights the importance of multifactor authentication for financial institutions with Internet-based services. In the guidance, the FFIEC states that single-factor authentication, as the only control mechanism, is inadequate for high-risk transactions involving access to customer information or the movement of

CEO QUESTIONS
Questions bank CEOs should ask

- How effective are my institution's policies and procedures for monitoring information inventory?
- Do my IT personnel have the appropriate knowledge or skills to protect against a potential cyber-attack?
- Is my staff informed about cyber threats? Do they have an understanding of risk from their actions?

funds to other parties. Financial institutions are advised to implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate risks.

An effective authentication system is necessary for compliance with requirements to safeguard customer information in the **Gramm-Leach-Bliley Act** to prevent money laundering and terrorist financing, to reduce fraud, to inhibit identity theft, and to promote the legal enforceability of electronic agreements and transactions. The risks of doing business with unauthorized or incorrectly identified persons in an Internet banking environment can result in financial loss and reputation damage through fraud, disclosure of customer information, corruption of data, or unenforceable agreements. More information is available in the FFIEC's *Authentication in an Internet Banking Environment* guide at http://www.ffiec.gov/pdf/authentication_guidance.pdf.

Access Controls

Identify and separate your most sensitive and critical information assets, such as your crown jewels, from less sensitive assets and establish multiple layers of security to access these critical information assets. In several high-profile breaches in recent years, attackers were able to gain access to sensitive data stored on the same servers with the same level of access as far less important data. Separating your crown jewels from less sensitive assets provides mitigation against data compromise.

Cybersecurity Staff Training Resources

- The FDIC created "Cyber Challenge: A Community Bank Cyber Exercise" to encourage community banks to conduct short exercises or facilitated discussions around four operational risk-related scenarios. The "Cyber Challenge" is available at https://www.fdic.gov/regulations/resources/director/technical/cyber/cyber.html.
- The National Cyber Security Alliance's Stay Safe Online website highlights topics management should talk to staff about regarding cybersecurity. These topics are available online at http://www.staysafeonline.org/business-safe-online/train-your-employees#sthash.6Rk0YSpN.dpuf.
- The Small Business Association provides a free training course on cybersecurity for small businesses. You can access their training course at http://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses.
- SANS offers a two-day security awareness training course called, "Securing The Human" that teaches key concepts and skills for changing employee behavior and reducing risk. The training uses a framework based on the Top 20 Critical Security Controls. More information on the training is available at http://www.securingthehuman.org/enduser.

Establish a process to track, control, prevent, correct, and secure access to your crown jewels and other assets, and decide which employees have a need and right to access these information assets. By controlling access to network resources, you can restrict unhealthy or misconfigured network clients from gaining entrance. If you place your resources in a shared cloud infrastructure, the provider must have a means of preventing inadvertent access.

Data Security

The loss of control over protected or sensitive data is a serious threat to business operations and a potential threat to national security. Protect your bank's data by using data loss prevention techniques. Not only is this a *Top 20 Critical Security Control*, banking regulators have issued regulations and supervisory guidance emphasizing the obligation of financial institutions to protect customer information. Interagency security guidelines implementing sections of the Gramm-Leach-Bliley Act and the **Fair and Accurate Credit Transactions Act of 2003** state financial institutions must:

- Develop and maintain an effective information security program tailored to the complexity of its operations; and
- Require, by contract, service providers that have access to its customer information to take appropriate steps to protect the security and confidentiality of this information.

CRITICAL SECURITY CONTROL #17

Data Protection: The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

For organizations that are moving data to the cloud, it is important to understand the security controls applied to data in the cloud environment and determine the best course of action for application of encryption controls. More information on the Council on CyberSecurity and the *Top 20 Critical Security Controls* is available at http://www.counciloncybersecurity.org/about-us/.

Data Encryption

Protect your bank's critical information assets by using data encryption tools. Data encryption tools are used to protect sensitive data in transit over communications networks or at rest in storage. These tools should be considered your first line of defense from cyber threats. Keep in mind, however, that even when encryption is used, there is always the risk that a sophisticated hacker can exploit vulnerabilities in the encryption algorithm or attack underlying processes and protocols.

Wireless Network

If your bank provides a wireless network for customers in your physical branches or offices, ensure that the public network is separate from the bank's private network and that all staff-connected devices with critical data are connected solely to the private network. Make sure that your private network is secure, and make sure Internet-connected devices to the private network have the appropriate antivirus and anti-malware protections in place. **The U.S. Computer Emergency Readiness Team (US-CERT)** provides a checklist covering basic steps to secure a wireless network at https://www.us-cert.gov/ncas/tips/ST05-003.

Additionally, talk with your IT manager or your vendor about protection for all pages on your public-facing website and mobile apps, not just the login portal. Vulnerabilities can occur through web pages and access points that do not seem to be vulnerable at first glance.

Finally, talk with your regulator about best practices for securing sensitive data. Many federal and state regulatory authorities now proactively engage financial institutions about their cybersecurity preparedness and may have time-sensitive resources for you to use.

Secure Configurations for Hardware and Software Systems

Ensure your IT staff has established, implemented, and is actively managing (tracking, reporting on, correcting) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

As delivered by manufacturers and resellers, the default configurations for operating systems and applications are normally geared to ease-of-deployment and ease-of-use, not security. Basic controls, open services and ports, default accounts or passwords, older (vulnerable) protocols, and pre-installation of unneeded software can all be exploitable in their default state.

The Council on CyberSecurity's recommended practices for securing configurations of hardware and software include:

- Establishing the use of standard secure configurations for your operating systems, ensuring to remove all unnecessary accounts, and disabling or removing unnecessary services.
- Implementing automated patching tools and processes for both applications and operating system software.
- Limiting administrative privileges to very few users who have both the knowledge necessary to administer the operating system and a business need to modify the configuration.

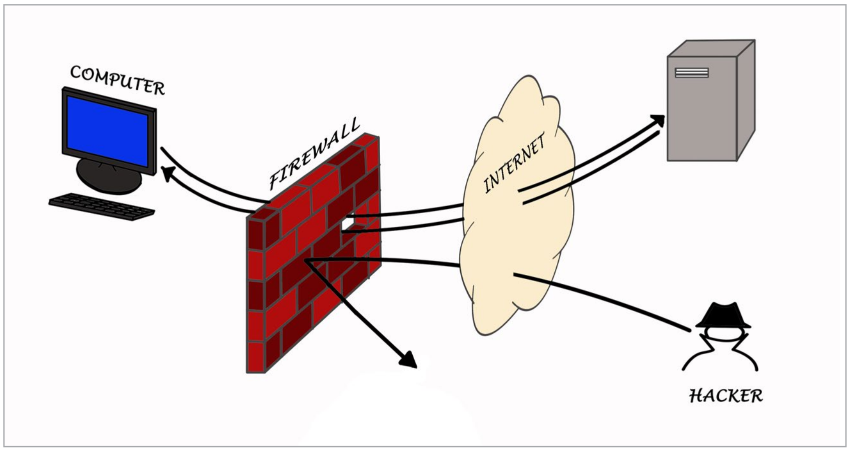
The Council on CyberSecurity also recommends that instead of starting from scratch, start from publicly developed and supported security benchmarks, security guides, or checklists. Some resources include the Center for Internet Security Benchmarks Program at www.cisecurity.org and the NIST National Checklist Program at checklists.nist.gov.

Perimeter Protection with a Firewall

A **firewall** is one of the most common tools used today to protect small and large businesses from intruders. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is assumed not to be secure and trusted. This is often referred to as "protecting the edge."

A firewall examines electronic data coming in or out of a network (or computer) and compares each piece of data to the security parameters it has been given. If it matches the rules, it is allowed to pass. If not, it is blocked and the system administrator is notified. In other words, firewalls provide broader protection against outside attackers by shielding your computer or network from malicious or unnecessary Internet traffic.

Figure 3. Firewall Diagram



Source: Conference of State Bank Supervisors

A firewall can either be software-based or hardware-based. According to the US-CERT, hardware-based firewalls are particularly useful for protecting multiple computers, but also offer a high degree of protection for a single computer. One advantage hardware-based firewalls have over software-based firewalls is that hardware-based firewalls are separate devices running their own operating systems. This way they provide an additional line of defense against attacks. The drawback to hardware-based firewalls is the additional cost, but there are many available for less than $100.

Software-based firewalls come built-in to some operating systems. The advantage of software-based firewalls is you can obtain one for relatively little or no cost. Because of the risks associated with downloading software from the Internet onto an unprotected computer, it is best to install the firewall from a CD or DVD. The disadvantage to a software firewall is that it is located on the same computer as the information you're trying to protect. This does provide some protection, but being located on the same computer may hinder the firewall's ability to catch malicious traffic before it enters your system.

Always remember that firewalls alone will not give you complete protection from cyber threats. However, using a firewall in conjunction with other protective measures and practices (such as anti-virus software and "safe" cyber hygiene) will strengthen your resistance to attacks.

DETECT

CYBERSECURITY 101

DETECT

If the cybersecurity protection tools covered in the PROTECT section are your banks "first line" of defense against Internet threats, consider the DETECT section tools as your reinforcement.

Cyber-attackers will attempt to exploit vulnerabilities that they can find, and it's up to your IT staff to detect such intrusions inside and outside of your network. To effectively do this, your IT manager must first have a thorough understanding of what is in your asset inventory and the associated risks (see IDENTIFY Section). Your IT manager should also ensure the appropriate safeguards are in place to protect your banks assets (see PROTECT Section).

The start of any detection strategy is the baseline inventory. Additionally, monitor your networks, systems, and applications to establish a baseline traffic pattern or establish a measure for "normal" operations. Your detection tools, which will be discussed later in this section, will then monitor for deviations from that normal state of activity. Your IT manager should also have a process in place for correcting any issues as you detect them.

Monitoring Deviations from Normal Operations

To mitigate threats proactively, use controls and sensors that automatically work to prevent or limit unauthorized access to computer networks, systems, or information. These may include:

- Intrusion Detection Systems;
- Network Behavior Anomaly Detection Tools;
- Security Information and Event Management /Log Analyzer;
- Configuration Management Tools; and
- Integrity Monitoring Tools.

Intrusion detection systems are security products that gather and analyze information from various areas within a computer or a network to identify possible security breaches, which include both intrusions from outside and inside the organization. These systems detect the occurrence of anomalies or cybersecurity incidents at your bank, enabling timely responses to a cyber-attack and the potential to limit or contain the impact of the attack.

CEO QUESTIONS

Questions bank CEOs should ask:

1. How is our executive leadership informed about the current level and business impact of cyber risks to our company?
2. Are we prepared to prevent or limit the damage caused by these attacks?

Network behavior anomaly detection tools, or NBAD, is a type of network security threat detection system that continuously monitors a network for unusual events or trends. NBAD tools offer added security in addition to that provided by other anti-threat applications such as firewalls, antivirus software, and spyware-detection tools. This is done by tracking critical network characteristics in real time and generating an alarm if an anomalous event is detected that could indicate the presence of a threat, such as larger than normal traffic volume to the website or bandwidth usage.

Security information and event management (SIEM) systems are tools used to manage logs and alerts from multiple security applications and devices. SIEM tools typically provide real-time monitoring, correlation of events, notifications, long-term storage, analysis, and reporting of log data.

A configuration management tool is predominantly a compliance configuration tool that provides a detailed recording of system or network configuration information for an organization's hardware and software. This information includes the versions and updates that have been applied to installed software packages and the locations and network addresses of hardware devices. Through periodic configuration scans the tool can detect any unplanned or unauthorized configuration changes or compliance anomalies and can highlight potential security threats.

It is essential that you learn from your detection activities by analyzing recurring or high-impact incidents or malfunctions. Additionally, to remain effective, these detection tools and associated processes must be regularly upgraded to enable continuous monitoring and real-time detections of constantly evolving threats.

CYBER THREATS

With innovation in technology has come the evolution of methods to deliver financial services. The industry has gone from the widespread use of ATMs in the 1980s, to modern point of sale (PoS) terminals in the 1990s, to Internet banking in the 2000s and mobile banking in 2010s. These new and evolving ways of meeting consumer demand, however, come with new fraud patterns and evolving risks of cyber-attacks.

Common cyber-attacks that bank CEOs should particularly know about and understand are:

- Distributed Denial of Service (DDoS) attacks;
- Corporate Account Take Over (CATO) attacks;
- Automated Teller Machine (ATM Cash Out) attacks; and
- CryptoLocker attacks.

Distributed Denial of Service (DDoS)

DDoS is a type of attack that attempts to make an online service unavailable by overwhelming a website with excessive traffic from multiple sources that interrupts normal services. In the latter half of 2012, an increased number of DDoS attacks were launched against financial institutions by politically motivated groups. These DDoS attacks have increased in sophistication and intensity. They have caused slow website response times, intermittently prevented customers from accessing institutions' public websites, and adversely affected back-office operations.

DDoS attacks are a threat to financial institutions of all sizes. Banks subject to a DDoS attack may face a variety of risks, including operational risks and reputation risks. The attack may also serve as a distraction while hackers attempt alternative types of fraud.

More information on DDoS attacks and how to mitigate this risk is available at: http://www.ffiec.gov/press/PDF/FFIEC%20DDoS%20Joint%20Statement.pdf.

Corporate Account Take Over (CATO)

CATO is a type of business identity theft where cyber-thieves impersonate the business and send unauthorized wire and ACH transactions to accounts controlled by the thieves. All businesses are vulnerable to a CATO attack, especially those with limited or non-existent computer safeguards and minimal or no disbursement controls for use with their bank's online business banking system. Losses from this form of cyber-crime have the potential to be substantial, with the majority of these thefts never being fully recovered. These thefts have affected both large and small banks.

The Conference of State Bank Supervisors (CSBS) joined with the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the U.S. Secret Service to create standards and best practices for mitigating the risks of Corporate Account Takeover. These industry-developed best practices have been in use in Texas since January 2012, where they have been well-received and welcomed by the banking industry. In addition to these best practices, several tools are available on CATO threats on the CSBS website. These include a sample risk assessment, sample notice of fraudulent activity, and law enforcement links.

More information and resources on CATO is available at: http://www.csbs.org/ec/cato/Pages/cato.aspx.

ATM Cash Out

ATM Cash Out is a type of large dollar-value ATM cash-out fraud characterized as Unlimited Operations by the U.S. Secret Service. Recently, there has been an increase in these types of cyber-attacks where thieves gain access to and alter the setting on ATM web-based control panels used by small- to medium-sized financial institutions.

ATM Cash Outs may cause financial institutions to incur large-dollar losses. Therefore, state and federal regulators expect financial institutions to take steps to address this threat by reviewing the adequacy of their controls over their information technology networks, card issuer authorization systems, systems that manage ATM parameters, and fraud detection and response processes.

More information on ATM Cash Out is available at: http://www.ffiec.gov/press/PDF/FFIEC%20ATM%20Cash-Out%20Statement.pdf.

CryptoLocker

CryptoLocker is a type of computer software malware or "ransomware" that emerged in 2013.
The malware is typically spread through phishing emails containing malicious attachments. Once a computer is infected, the malware encrypts the data, thereby restricting access to the data on the infected computers. Then the malware demands the victim provide a payment (or ransom) to the attackers in order to decrypt and recover their files.

The malware has the ability to find and encrypt files located within shared network drives, USB drives, external hard drives, network file shares, and even some cloud storage drives. If one computer on a network becomes infected, mapped network drives could also become infected. While victims are told they have three days to pay the attacker through a third-party payment method (i.e. MoneyPak, Bitcoin), some victims have claimed online that they paid the attackers and did not receive the promised decryption key. The U.S. Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) encourages users and administrators experiencing a ransomware infection to report the incident to the FBI at the Internet Crime Complaint Center at: http://www.ic3.gov/default.aspx. More information on CryptoLocker is available at: https://www.us-cert.gov/ncas/alerts/TA13-309A.

EIGHT MOBILE BANKING SECURITY RECOMMENDATIONS

The use of mobile banking has increased substantially in recent years, and studies show this trend is very likely to continue as more consumers opt for the convenience of mobile technology. In 2012, 33 million U.S. consumers used their mobile devices to conduct financial transactions, and according to Aite Group, an independent research and advisory firm, an estimated 96 million U.S. consumers will adopt mobile banking by 2016. To keep up with the rise in consumer demand, Aite expects the number of financial institutions offering mobile banking solutions to their retail banking customers will also increase.

As demand for the convenience of mobile banking continues to grow, so too has concern regarding the security of mobile banking applications. A report published by Deloitte Center for Financial Services in May 2014 revealed that a leading reason some smartphone users do not engage in mobile banking is concern regarding the security of the applications. The Deloitte report is available at http://dupress.com/articles/mobile-financial-services/.

Mobile banking has opened a new door for cybercriminals, and the ecosystem of mobile banking involves several players which can be challenging when addressing issues of security. These players include customers, merchants, banks, debit/credit card networks, clearing/settlement organizations, application providers, third-party payment providers, wireless carriers, and handset/chip manufacturers, all of which are responsible for some level of security. For banks, there are various measures that can be taken to address the security of mobile banking and payments.

Additional recommendations for a secure transition to mobile banking is available in an executive financial services report by Symantec titled, "Banks Likely to Remain Top Cybercrime Targets." It's available for download at http://www.symantec.com/content/en/us/enterprise/other_resources/b_Financial_Attacks_Exec_Report.pdf.

EIGHT MOBILE BANKING SECURITY RECOMMENDATIONS

01 Communication by the mobile banking app through the Internet should employ secure transmission protocols, such as Hypertext Transfer Protocol Secure (HTTPS), which is more difficult to hack;

02 Customer data exchanged with third-party vendors should be encrypted (in transmission and storage);

03 PINs required in the mobile application should not be less than 6 characters;

04 There should be dual authentication for log-in credentials;

05 Applications should time out after at most 15 minutes of inactivity;

06 There should be real-time application monitoring;

07 “Jail-broken” devices should not be allowed on the network; and

08 Heightened diligence should be taken to ensure the security and compliance of vendors.

Sources:

Deloitte Center for Financial Services. Mobile Financial Services: Raising the Bar on Customer Engagement. (2014). Retrieved from http://dupress.com/articles/mobile-financial-services/.

Federal Financial Institutions Examinations Council. IT Examination Handbook. Retrieved from http://ithandbook.ffiec.gov/it-booklets/e-banking/appendix-e-wireless-banking.aspx.

Pegueros, Vanessa (2012). Security of Mobile Banking and Payments. SAN Institute Info Sec Reading Room. Retrieved from http://www.sans.org/reading-room/whitepapers/ecommerce/security-mobile-banking-payments-34062.

Symantec. Executive Report: Financial Services: Banks Likely to Remain Top Cybercrime Targets. Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b_Financial_Attacks_Exec_Report.pdf.

RESPOND

CYBERSECURITY 101

RESPOND

Cybersecurity data breaches are now part of our way of life. Even large, well-funded, and technically sophisticated institutions struggle to keep up with the frequency and complexity of cyber-attacks. Even still, it is important that banks adequately prepare for a cybersecurity incident, and this includes knowing how you will respond once an incident occurs. To do this, banks must have an incident response plan.

Where to Start in Developing an Incident Response Plan

1. Start with creating your incident response team. Coordinate efforts between your bank's various departments or roles to determine the team members. This process should include the CEO, the head of IT, legal personnel, human resources, and the head of communications.

2. Select a leader for the incident response team and identify the members of the senior management team who can declare an incident.

3. Outline a structure of internal reporting to ensure executives and everyone on the response team is up-to-date and on-track during a data breach.

4. Clearly define steps, timelines, and checklists to keep the team focused during the stress of a data breach.

5. Conduct preparedness training for the incident response team.

The Incident Response Plan

At a minimum, your bank's incident response plan should address the following issues:

- How to address potential damage and limit loss of resources.

- Whether evidence needs to be preserved. For more information, see *NIST Chain of Custody Sample*: http://www.nist.gov/oles/forensics/upload/Sample-Chain-of-Custody-Form.docx.

- Criterion when special forensics may be required. Digital evidence forensic is a very specialized activity. Organizations usually outsource this function to specialized forensics labs. For more information see NIST SP 800-86 http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

- How service availability is affected, such as network connectivity or services provided to external parties.

- The time and resources needed to implement the strategy.

- The effectiveness of the strategy; that is, whether it partially or fully contains the incident.

- How long remediation solutions are intended to last. For example, an emergency workaround might need to be removed after some period of time, or a solution might be permanent.

CEO QUESTIONS

Questions bank CEOs should ask:

- Have we created an effective incident response plan? How often is it tested?

- What would we do if we were hacked today?

- Do we have a plan to inform internal and external stakeholders?

Communicating a Data Breach

Your bank's incident response plan should also address communicating a data breach to customers, regulators, law enforcement, and other stakeholders. When informing stakeholders about a data breach, your bank's incident response plan should generally include the following:

- When and if you should report a breach to the media and/or notify affected individuals;
- Which medium is the best for notifying stakeholders;
- Key messaging; and
- Basic guidelines for tracking and analyzing media coverage as a result of the breach.

Depending on the type of data compromised, you may have a legal obligation to inform your customers. This is likely the case if personal information or financial data have been breached. A resource for state-by-state laws on data breach notification requirements is available by the Baker & Hostetler LLP law firm at http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf. Bank CEOs are encouraged to check with their state regulator, however, as laws on disclosures differ from state to state and change from year to year.

A comprehensive guide on forming and executing an incident response plan is available from Experian Data Breach Resolution at http://www.experian.com/assets/data-breach/brochures/response-guide.pdf. The guide also covers legal considerations when experiencing a data breach, such as mandatory state notification laws, a template notification letter to customers, and best practices for negotiating security safeguards with vendors.

You've Been Hacked/Attacked, What Are Your Next Steps?

The following are three steps bank CEOs should consider when responding to a cybersecurity incident:

- Triage/Evaluate the Cyber-event;
- Invoke the Incident Response Plan; and
- Review the 24-Hour Checklist.

Triage/Evaluate the Cyber-Event

After receiving notification of a potential cybersecurity event, evaluate the event by answering critical questions, such as were high-value assets compromised? Were any data altered?

CRITICAL SECURITY CONTROL #18

Incident Response and Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g. plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

More information on the Council on Cybersecurity and the Top 20 Critical Security Controls is available at http://www.counciloncybersecurity.org/about-us/.

Invoke the Incident Response Plan

Once it is determined that a cybersecurity event has occurred, carry out the cybersecurity incident response plan. Please note that by the time a cyber-attack occurs, it is often too late to develop the right procedures. Create and implement a security incident response plan now to better prepare for a cyber-attack later.

The First 24 Hours Checklist

It's been discovered that your bank has been hacked or attacked. What should you do? Once you have detected a cyber-incident, immediately contact your legal counsel for guidance on initiating these ten steps:

1. **Record the date and time** when the breach was discovered, as well as the current date and time when response efforts begin, i.e. when someone on the response team is alerted to the breach.

2. **Alert and activate everyone** on the response team, including external resources, to begin executing your preparedness plan.

3. **Secure the premises** around the area where the data breach occurred to help preserve evidence, if necessary.

4. **Stop additional data loss.** Take affected machines or servers offline.

5. **Document everything** known about the breach. Who discovered it? Who reported it? To whom was it reported? Who else knows about it? What type of breach occurred? What was stolen? How was it stolen? What systems are affected? What devices are missing?

6. **Interview those involved** in discovering the breach and anyone else who may know about it. Document your investigation.

7. **Review protocols** regarding disseminating information about the breach for everyone involved in this early stage.

8. **Assess priorities and risks** based on what you know about the breach.

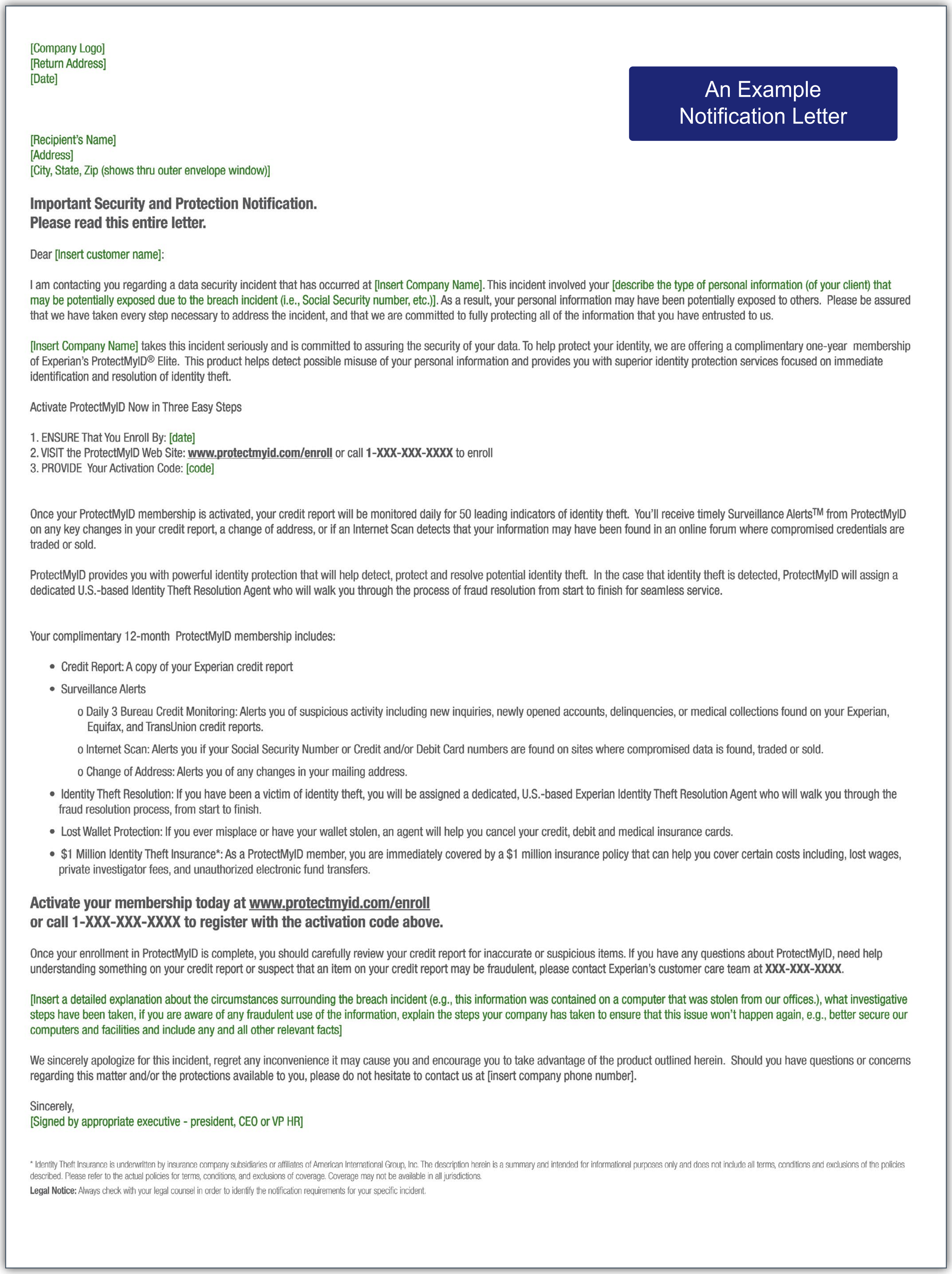
9. **Inform the proper authorities**, including your banking regulator, the U.S. Secret Service or the Federal Bureau of Investigation.

10. **Notify law enforcement**, if needed, to begin an in-depth investigation.

For more information on forming and executing an incident response plan, here are two guides that provide best practices to follow:

- *Data Breach Response Guide* by Experian Data Breach Resolution at: http://www.experian.com/assets/data-breach/brochures/response-guide.pdf; and

- *Cyber Incident Response Guide* published by the Multi-State Information Sharing & Analysis Center at: https://msisac.cisecurity.org/resources/guides/documents/Incident-Response-Guide.pdf.



[Company Logo]
[Return Address]
[Date]

An Example Notification Letter

[Recipient's Name]
[Address]
[City, State, Zip (shows thru outer envelope window)]

Important Security and Protection Notification.
Please read this entire letter.

Dear [Insert customer name]:

I am contacting you regarding a data security incident that has occurred at [Insert Company Name]. This incident involved your [describe the type of personal information (of your client) that may be potentially exposed due to the breach incident (i.e., Social Security number, etc.)]. As a result, your personal information may have been potentially exposed to others. Please be assured that we have taken every step necessary to address the incident, and that we are committed to fully protecting all of the information that you have entrusted to us.

[Insert Company Name] takes this incident seriously and is committed to assuring the security of your data. To help protect your identity, we are offering a complimentary one-year membership of Experian's ProtectMyID® Elite. This product helps detect possible misuse of your personal information and provides you with superior identity protection services focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE That You Enroll By: [date]
2. VISIT the ProtectMyID Web Site: **www.protectmyid.com/enroll** or call **1-XXX-XXX-XXXX** to enroll
3. PROVIDE Your Activation Code: [code]

Once your ProtectMyID membership is activated, your credit report will be monitored daily for 50 leading indicators of identity theft. You'll receive timely Surveillance Alerts™ from ProtectMyID on any key changes in your credit report, a change of address, or if an Internet Scan detects that your information may have been found in an online forum where compromised credentials are traded or sold.

ProtectMyID provides you with powerful identity protection that will help detect, protect and resolve potential identity theft. In the case that identity theft is detected, ProtectMyID will assign a dedicated U.S.-based Identity Theft Resolution Agent who will walk you through the process of fraud resolution from start to finish for seamless service.

Your complimentary 12-month ProtectMyID membership includes:

- Credit Report: A copy of your Experian credit report
- Surveillance Alerts
  - Daily 3 Bureau Credit Monitoring: Alerts you of suspicious activity including new inquiries, newly opened accounts, delinquencies, or medical collections found on your Experian, Equifax, and TransUnion credit reports.
  - Internet Scan: Alerts you if your Social Security Number or Credit and/or Debit Card numbers are found on sites where compromised data is found, traded or sold.
  - Change of Address: Alerts you of any changes in your mailing address.
- Identity Theft Resolution: If you have been a victim of identity theft, you will be assigned a dedicated, U.S.-based Experian Identity Theft Resolution Agent who will walk you through the fraud resolution process, from start to finish.
- Lost Wallet Protection: If you ever misplace or have your wallet stolen, an agent will help you cancel your credit, debit and medical insurance cards.
- $1 Million Identity Theft Insurance*: As a ProtectMyID member, you are immediately covered by a $1 million insurance policy that can help you cover certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Activate your membership today at www.protectmyid.com/enroll
or call 1-XXX-XXX-XXXX to register with the activation code above.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at **XXX-XXX-XXXX**.

[Insert a detailed explanation about the circumstances surrounding the breach incident (e.g., this information was contained on a computer that was stolen from our offices.), what investigative steps have been taken, if you are aware of any fraudulent use of the information, explain the steps your company has taken to ensure that this issue won't happen again, e.g., better secure our computers and facilities and include any and all other relevant facts]

We sincerely apologize for this incident, regret any inconvenience it may cause you and encourage you to take advantage of the product outlined herein. Should you have questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact us at [insert company phone number].

Sincerely,
[Signed by appropriate executive - president, CEO or VP HR]

* Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Legal Notice: Always check with your legal counsel in order to identify the notification requirements for your specific incident.

RECOVER

CYBERSECURITY 101

RECOVER

Restore & Review

After your bank has taken the necessary action to respond to a cyber-attack, the next step is the recovery period. Develop and implement a recovery plan that includes appropriate processes and procedures for how you intend to restore confidence in your recovered systems and data.

Your recovery plan may include the following:

- **Recover Infrastructure:** A step-by-step plan for rebuilding servers, databases, network devices that may have been compromised, and restoring baseline configurations. Your IT staff should maintain a standard set of up-to-date infrastructure images that are ready to install—for example, using a virtual machine or USB flash drive.

- **Restore Data**: If the integrity of data was impacted or content deleted, have a plan in place for restoring it. Your IT staff should have a reliable backup procedure in place.

- **Reconnect Service:** Your recovery plan should lay out how you will reconnect services with minimum disruption.

In some cases it may take weeks to restore normal operations, as you may need to deploy a new technology or service. In other cases it may take hours. It all depends on the impact of the cyber-incident. Using the information you learned about the cyber-attack, identify and eliminate the vulnerabilities exploited by the attacker to protect against future attacks.

Once impaired systems are restored and back online, the cyber-incident response team should:

- Determine what cybersecurity management improvements are necessary to prevent similar attacks from occurring;

- Review the team's execution of the incident response plan; and

- Consider whether the incident response plan can be improved;

Preparedness Plan Audit

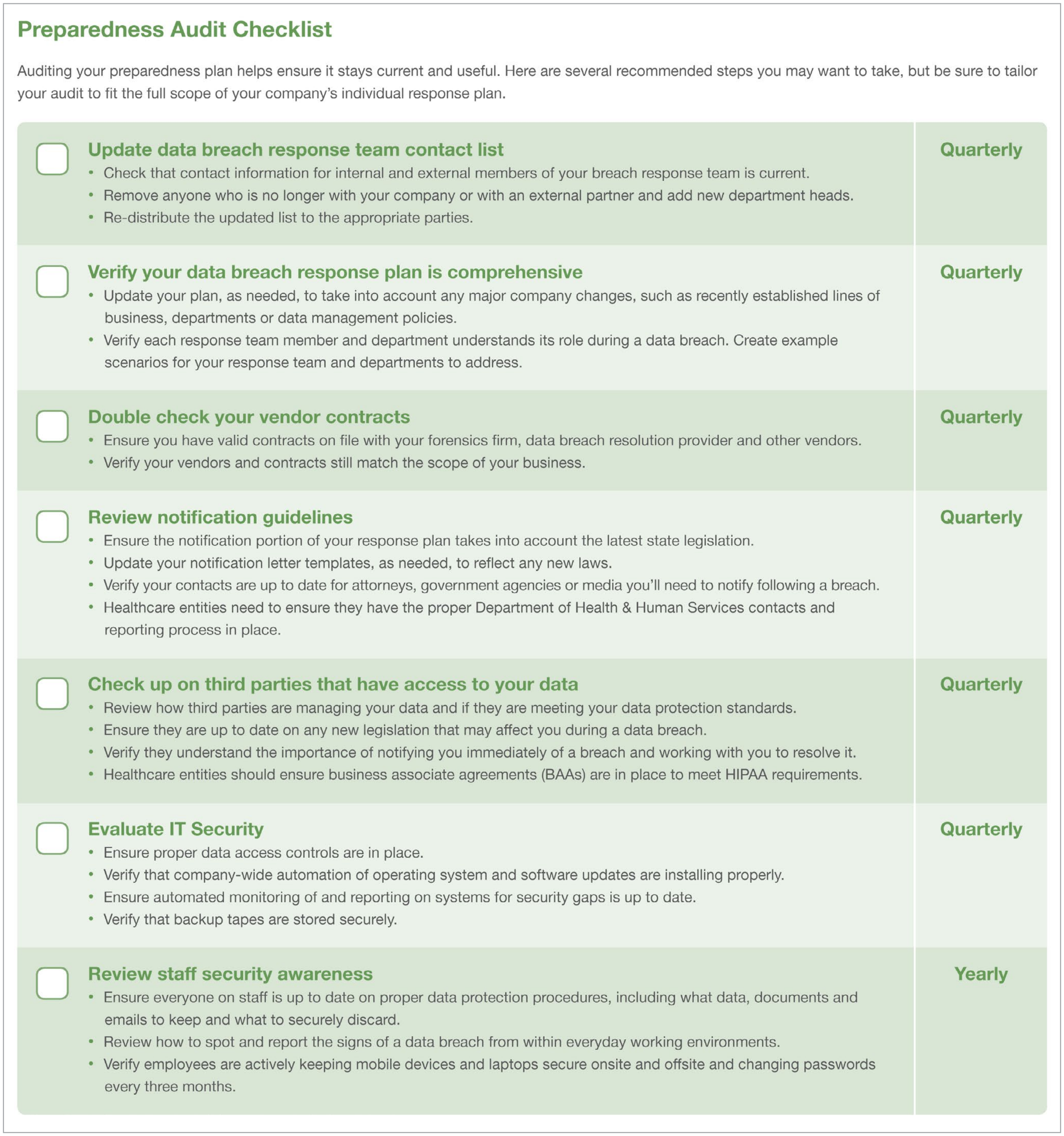
It's not enough to simply have an incident response plan. With the increasingly sophisticated and evolving cyber threats that exist today, your management team should routinely audit and test your plan to ensure it remains current and useful. Figure 4 shows recommended steps by Experian Data Breach Resolution that you may want to take when auditing your incident response plan. As these are general recommended steps, be sure to tailor them to fit the full scope of your bank's individual incident response plan.

CEO QUESTIONS

Questions bank CEOs should ask:

- Does my bank's incident response plan include steps for recovering after a cyber-attack?
- When did we last test our incident response plan?
- How will we communicate with internal staff, customers, third parties, regulators and law enforcement of a data breach at my financial institution?

Figure 4. Preparedness Audit Checklist



Preparedness Audit Checklist

Auditing your preparedness plan helps ensure it stays current and useful. Here are several recommended steps you may want to take, but be sure to tailor your audit to fit the full scope of your company's individual response plan.

□	**Update data breach response team contact list** • Check that contact information for internal and external members of your breach response team is current. • Remove anyone who is no longer with your company or with an external partner and add new department heads. • Re-distribute the updated list to the appropriate parties.	**Quarterly**
□	**Verify your data breach response plan is comprehensive** • Update your plan, as needed, to take into account any major company changes, such as recently established lines of business, departments or data management policies. • Verify each response team member and department understands its role during a data breach. Create example scenarios for your response team and departments to address.	**Quarterly**
□	**Double check your vendor contracts** • Ensure you have valid contracts on file with your forensics firm, data breach resolution provider and other vendors. • Verify your vendors and contracts still match the scope of your business.	**Quarterly**
□	**Review notification guidelines** • Ensure the notification portion of your response plan takes into account the latest state legislation. • Update your notification letter templates, as needed, to reflect any new laws. • Verify your contacts are up to date for attorneys, government agencies or media you'll need to notify following a breach. • Healthcare entities need to ensure they have the proper Department of Health & Human Services contacts and reporting process in place.	**Quarterly**
□	**Check up on third parties that have access to your data** • Review how third parties are managing your data and if they are meeting your data protection standards. • Ensure they are up to date on any new legislation that may affect you during a data breach. • Verify they understand the importance of notifying you immediately of a breach and working with you to resolve it. • Healthcare entities should ensure business associate agreements (BAAs) are in place to meet HIPAA requirements.	**Quarterly**
□	**Evaluate IT Security** • Ensure proper data access controls are in place. • Verify that company-wide automation of operating system and software updates are installing properly. • Ensure automated monitoring of and reporting on systems for security gaps is up to date. • Verify that backup tapes are stored securely.	**Quarterly**
□	**Review staff security awareness** • Ensure everyone on staff is up to date on proper data protection procedures, including what data, documents and emails to keep and what to securely discard. • Review how to spot and report the signs of a data breach from within everyday working environments. • Verify employees are actively keeping mobile devices and laptops secure onsite and offsite and changing passwords every three months.	**Yearly**

Source: Experian Data Breach Resolution's Data Breach Response Guide, 2013-2014

Test Your Incident Response Plan

In addition to auditing, test your incident response plan annually. You may do this by conducting *tabletop exercises*, which are facilitated, discussion-based exercises where staff meets to discuss roles, responsibilities, coordination, and decision-making of a given scenario. Another exercise you may conduct to test the incident response plan includes a *functional exercise*, where your staff validates its readiness for emergencies by performing duties in a simulated environment. Whether you conduct a tabletop or functional exercise, the goal should be to evaluate established policies and procedures of the current incident response plan and staff readiness.

Engage Third-Party Vendors

One recommendation on the audit checklist is to check up on third parties that have access to your bank's data. You will want to ensure your vendors have appropriate security measures in place for the data they will process. Consider contractually obligating your vendors to maintain sufficient data safeguards and assess whether they are meeting the contract requirements on a regular basis.

In general, it makes sense for financial institutions to require that vendors:

- Maintain a written security program that covers your bank's data;
- Only use your bank's data for the sole purpose of providing the contracted services;
- Promptly notify your bank of any potential security incidents involving company data and cooperate with your bank in addressing the incident;
- Comply with applicable data security laws. Ensure the vendor is up to date on any new legislation that may affect your bank during a breach; and
- Return or appropriately destroy company data at the end of the contract.

While today's recommended practices and technology tools may go a long way to secure financial institutions from potential Internet threats, the rise in the number of cyber-attacks that have occurred in recent years illustrate more is still needed to protect against cyber-attacks. But with the financial services industry, along with state and federal regulators working together, we increase our ability to continue finding better ways of supporting enhanced resistance, resiliency, and a shared understanding of the many cyber risks that exist today and beyond.

GLOSSARY

Council on Cybersecurity – Aims to accelerate the widespread availability and adoption of effective cybersecurity measures, practice, and policy.

Controlled Access – Minimum set of security functionally that enforces access control on individual users and makes them accountable for their actions through log-in procedures, auditing of security-relevant events, and resource isolation.

Crown Jewels – Critical information assets that are regarded as highly sensitive, essential pieces of information to the organization.

Cyber-attack – An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Cyber Hygiene – Refers to steps computer users take to protect and maintain systems and devices.

Cybersecurity – The ability to protect or defend the use of cyberspace from cyber-attacks.

Cybersecurity and Critical Infrastructure Working Group (CCIWG) – In June 2013 the FFIEC established this body to enhance communication among the FFEIC member agencies and build on existing efforts to strengthen the activities of other interagency and private sector groups.

Cybersecurity Inherent Risk – The amount of risk posed by a financial institution's activities and connections, notwithstanding risk-mitigating controls in place. A financial institution's cybersecurity inherent risk incorporates the type, volume, and complexity of operational considerations, such as connection types, products and services offered, and technologies used.

Data Loss – The exposure of proprietary, sensitive, or classified information through either data theft or data leakage.

Data Security – Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.

Distributed Denial of Service (DDoS) – The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

Fair and Accurate Credit Transactions Act of 2003 – Added sections to the federal Fair Credit Reporting Act, intended to help consumers fight the growing crime of identity theft.

Federal Financial Institutions Examination Council (FFIEC) – A formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB), and to make recommendations to promote uniformity in the supervision of financial institutions. In 2006, the State Liaison Committee (SLC) was added to the Council as a voting member. The SLC includes representatives from the Conference of State Bank Supervisors (CSBS), the American Council of State Savings Supervisors (ACSSS), and the National Association of State Credit Union Supervisors (NASCUS).

Firewall – A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy.

Financial Services Information Sharing and Analysis Center (FS-ISAC) – A private-sector nonprofit information-sharing firm established by financial services industry participants in response to the federal government's efforts to facilitate the public and private sectors' sharing of physical and cybersecurity threat and vulnerability information.

Gramm-Leach-Bliley Act – Requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.

Incident Response Plan – The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attack against an organization's information system(s).

Infragard – FBI Infragard is a partnership between the FBI and the private sector. It is an association of people who represent businesses, academic institutions, state and local law enforcement agencies and other participants dedicated to sharing information and intelligence to prevent hostile acts against the U.S.

Intrusion Detection Prevention System (DPS) – Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.

Intrusion Detection System (IDS) – Hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations).

Multi-State Information Sharing & Analysis Center – A source for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments.

National Institute of Standards and Technology (NIST) – A non-regulatory federal agency within the U.S. Department of Commerce that aims to promote U.S. innovation and industrial competitiveness by advancing measurement, science, standards, and technology in ways that enhance economic security and improve quality of life.

NIST's Cybersecurity Framework – A set of industry standards and best practices to help organizations manage cybersecurity risks.

Risk – The potential for loss, damage, or destruction of an asset as a result of a threat exploiting vulnerability

Risk-Assessment – The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation, arising through the operation of an information system. Part of risk management, risk assessment incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

Symantec Corporation – An information protection company that makes security, storage, and backup software, and offers professional services.

Threat – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

Top 20 Critical Security Controls – A reference set of recommendations to address risks to company data and systems. Each year the Council on Cybersecurity, located in the Washington, D.C. area, releases its Top 20 Critical Security Controls. These controls are meant to establish priority of action for organizations actively managing cybersecurity risks and to keep knowledge and technology current in the face of rapidly evolving cyber threats.

U.S. Computer Emergency Readiness Team (US-CERT) – Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber-attacks across the nation.

U.S. Secret Service Electronic Crimes Task Force (ECTF) – Brings together not only federal, state, and local law enforcement but also prosecutors, private industry, and academia in the prevention, detection, mitigation, and investigation of attacks on the nation's financial and critical infrastructures.

Virtual Private Network – A virtual private network (VPN) extends a private network across a public network, such as the Internet.

Vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

SOURCES

Aite Group. *Mobile Banking Forecast: Smartphone and Tablet Use in the United States.* (2012). Retrieved from http://www.aitegroup.com/report/mobile-banking-forecast-smartphone-and-tablet-use-united-states#sthash.DoRXBMkv.dpuf.

Conference of State Bank Supervisors, FS-ISAC, U.S. Secret Service. *Corporate Account Takeover Initiative*. (2012). Retrieved from http://www.csbs.org/ec/cato/Pages/cato.aspx.

Council on CyberSecurity. *The Critical Security Controls for Effective Cyber Defense,* Version 5.0 (2014). Retrieved from http://www.counciloncybersecurity.org/.

Baker & Hostetler LLP. Data Breach Charts. (2014) Retrieved from http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf.

Deloitte Center for Financial Services. *Mobile Financial Services: Raising the Bar on Customer Engagement*. (2014). Retrieved from http://dupress.com/articles/mobile-financial-services/.

Department of Homeland Security. *Cybersecurity for Small and Medium-Sized Businesses and Entrepreneurs*. (September, 2014). Retrieved from http://www.dhs.gov/national-cyber-security-awareness-month-2014-week-four.

Department of Homeland Security U.S. Computer Emergency Readiness Team. Retrieved from https://www.us-cert.gov/ncas/tips.

EMC Corporation. *Realizing the Mobile Enterprise: Balancing the Risks and Rewards of Consumer Devices*. Retrieved from http://searchsecurity.techtarget.com/feature/BYOD-security-strategies-Balancing-BYOD-risks-and-rewards.

Experian Data Breach Resolution. *Data Breach Response Guide* (2013-2014). Retrieved from http://www.experian.com/assets/data-breach/brochures/response-guide.pdf.

Federal Financial Institutions Examinations Council. *Financial Regulators Release Statements on Cyber-Attacks on Automated Teller Machine and Card Authorization Systems and Distributed Denial of Service Attacks*. (April 2, 2014). Retrieved from http://www.ffiec.gov/press/pr040214.htm.

Federal Financial Institutions Examinations Council. *Executive Leadership of Cybersecurity: What Today's CEO Needs to Know about the Threats They Don't See*. (May 7, 2014). Retrieved from https://www.brainshark.com/csbs/vu?pi=zGBzRS8LMz3pQMz0&intk=905196563.

Federal Financial Institutions Examinations Council. *IT Risk Management Process*. Retrieved from http://ithandbook.ffiec.gov/it-booklets/management/it-risk-management-process.aspx.

He, Zhaozhao. (September 2014). *Rivalry, Market Structure and Innovation: The Case of Mobile Banking*. Retrieved from http://www.stlouisfed.org/banking/community-banking-conference-2014/content/pdfs/SESSION1_He.pdf.

MITRE. *Crown Jewels Analysis*. Retrieved from http://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis.

Multi-State Information Sharing & Analysis Center. *Cyber Incident Response Guide*. Retrieved from https://msisac.cisecurity.org/resources/guides/documents/Incident-Response-Guide.pdf.

Multi-State Information Sharing & Analysis Center. *Risk Management Guide*. Retrieved from https://msisac.cisecurity.org/resources/guides/documents/Risk-Management-Guide.pdf.

National Cyber Security Alliance. Stop, Think, Connect Campaign. *Keep a Clean Machine*. Retrieved from http://www.stopthinkconnect.org/campaigns/keep-a-clean-machine.

Pegueros, Vanessa (2012). *Security of Mobile Banking and Payments*. SAN Institute Info Sec Reading Room. Retrieved from http://www.sans.org/reading-room/whitepapers/ecommerce/security-mobile-banking-payments-34062.

Risk Based Security, Open Security Foundation. *Data Breach QuickView: An Executive's Guide to 2013 Data Breach Trends*. (February, 2014). Retrieved from https://www.riskbasedsecurity.com/reports/2013-DataBreachQuickView.pdf.

Schutzer, Dan (2014). *Cyber Security Trends.* BITS/ Financial Services Roundtable. Retrieved from http://www.bits.org/publications/CTO/CTOCornerMarch2014.pdf.

Securities Industry and Financial Markets Association. *Small Firm Cybersecurity Checklist*. Retrieved from http://www.sifma.org/uploadedfiles/issues/technology_and_operations/cyber_security/cybersecurity-small-firms-action-item-checklist.pdf?n=50189.

Symantec. *Executive Report: Financial Services: Banks Likely to Remain Top Cybercrime Targets.* Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b_Financial_Attacks_Exec_Report.pdf.

US-CERT. *CryptoLocker Ransomware Infections*. (November 5, 2013). Retrieved from https://www.us-cert.gov/ncas/alerts/TA13-309A.

US-CERT. *Securing Wireless Networks*. Retrieved from https://www.us-cert.gov/ncas/tips/ST05-003.

U.S. Small Business Administration. *Cybersecurity for Small Businesses.* Retrieved from http://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses.

CSBS SINCE 1902

CONFERENCE OF STATE BANK SUPERVISORS

1129 20th Street NW
Washington, D.C.

202-296-2840
*For questions or comments contact
the CSBS Communications Department.*