CSBS

CYBERSECURITY 101

A Resource Guide for Financial Sector Executives

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 FINANCIAL SECTOR EXECUTIVES THAT MANAGEMENT OF AN INSTITUTION'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

A Letter From the President and CEO

Colleagues,

I am proud to present to you the revised Conference of State Bank Supervisors (CSBS) Executive Leadership of Cybersecurity (ELOC) Resource Guide, or "Cybersecurity 101."

The number of cyber-attacks directed at financial institutions of all sizes continues to grow. Addressing new threats requires a concerted effort by Chief Executive Officers (CEOs), Presidents, and Board Members. Several years ago CSBS, on behalf of state regulators, launched the ELOC Initiative to engage bank executives and provide them with the tools to address cybersecurity threats.

Since its initial publication, "Cybersecurity 101" has served as a valuable resource for countless bank executives. In this update, however, you will notice several changes. Most notably, we removed previously included technical information, such as detailed instructions for activities performed by your IT and information security personnel. They will be incorporated into appendices and made available separately. The guide has also been updated to address both bank and nonbank institutions. We intend this document as a reference for both the banks that have formed the cornerstone of our economy for hundreds of years, as well as the emerging technologies shifting our industry in exciting and challenging ways.

This guide is tailored to furnish Executives with the necessary tools to better understand and prepare for the threats faced by their institutions.

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

Sincerely,

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

CONTENTS

Introduction 3

What Do We Mean When We Talk About Risk? 4

- Common Threats 5

Questions Every CEO Should Ask 6

How to Structure Your Information Security Program 7

- Identify 8
  - Identifying Threats 8
  - Measuring Risk 10
  - Communicating Risk 10
- Protect 12
- Detect 17
- Respond 18
- Recover 21

Glossary 22

Resources 23

INTRODUCTION

Financial institutions collect and protect highly sensitive information every day. The financial services industry is a vital component of the nation's critical infrastructure—banks and nonbank financial institutions are the cornerstones of local communities, intrastate commerce, and the U.S. economy.

As CEOs, Executives, and/or Board Members, you have the responsibility to adequately protect the money and information entrusted to you by your consumers; losing the trust of your employees and customers puts your institution at risk.

Cyber risks, like reputational and financial risks, threaten an institution's bottom line. Attacks can be costly and compromising to customer confidence, and the institution may even be held legally responsible. Beyond the impact to an individual organization, though, cyber-attacks also have far-reaching economic consequences. Due to the inherent interconnectedness of the internet, a security breach at one financial institution can pose a significant threat to market confidence and the nation's financial stability, as well as to other financial institutions. But in this time of technological advancement and interconnectedness, it can be challenging to know how to best defend your institutions. With limited resources, how can risks be prioritized?

This guide addresses challenges faced by both bank and nonbank (also referred to as "non-depository") institutions. It is intended as an easily digestible, non-technical reference guide to help executives develop a comprehensive, responsive cybersecurity program in line with best practices. As each institution is different, the advice in this guide can be easily customized to meet your organization's unique threats, priorities, and challenges. While this resource guide does not guarantee prevention, it attempts to identify various resources—people, processes, and tools and technologies—that, when properly leveraged, work to reduce your cybersecurity risk.

It is our hope that this guide serves as a starting point to sustained collaboration between financial institutions and regulators. Together we can safeguard against new, persistent cybersecurity threats and contribute to a stable, prosperous economy.

What Do We Mean When We Talk About Risk?

Risk is the likelihood and potential magnitude of harm. It lies at the nexus of two important information security concepts: **threats** and **vulnerabilities**.

A **threat** is a force, organization, or person with the potential to obtain, compromise, or destroy an information asset. Threats can be physical, like an employee accidentally deleting critical information; natural, like a tornado or earthquake; or internet-based, such as malicious software or viruses. It is important to remember your organization is not only threatened by bad actors, criminals, or acts of nature; **insider threats**, such as human error or disgruntled employees, must also be defended against. A **vulnerability**, or weakness, is a gap in information or physical security protections that can be exploited to cause harm or accident.

It is impossible to protect against all vulnerabilities. Every organization maintains some level of risk—it is the cost of doing business. Fortunately, implementing a robust cybersecurity program will reduce your organization's level of risk to an acceptable one. As an executive, it is your role to determine the level of risk—in accordance with the Board—palatable to your institution.

IT IS IMPOSSIBLE TO PROTECT AGAINST ALL VULNERABILITIES.

Common Threats

Phishing Attacks prey on a user's sense of responsibility, empathy, or urgency to trick him or her into sharing credentials with an unauthorized user, usually via email or telephone.

Insider Threats are threats posed by employees, vendors, and people close to the business, either on purpose or by accident.

Denial of Service Attacks are an attempt to overwhelm a website or tool with requests so that it becomes useless.

Ransomware Attacks encrypt valuable computer resources and hold them hostage until a ransom—often demanded in cryptocurrency—is paid.

Natural Disasters, like hurricanes, interrupt business operations and can deprive communities of access to financial resources.

Questions Every CEO Should Ask

Although cybersecurity was once considered solely an information technology (IT) concern, the increase in frequency and sophistication of cyber-attacks demands a shift in thinking. For a cyber program to be truly effective, it must involve the CEO, Board Members, and other senior executives in addition to information security and IT professionals.

CEOs should ask themselves several questions to determine their organizations' risk appetites.

1. **What internal and external threats do we face?**
2. **What are my organization's critical assets and information? Can I prioritize what's most important to continued business operations?**
3. **What information does my institution manage and where is it stored? Who has access to it?**
4. **Does my organization have a Chief Information Security Officer (CISO)? If not, who is responsible for cybersecurity?**
5. **Who is providing services to my organization? How do we ensure our vendors take care of their own information and ours?**
6. **Am I receiving the cybersecurity information I need to make active risk management decisions?**
7. **Am I routinely communicating relevant risk environment and risk management decisions to the Board?**
8. **How can my budget be optimized to address cybersecurity concerns?**

KNOW WHO TO ASK

Identify the cybersecurity professionals who work for you and their areas of expertise. They should be able to answer your questions and provide feedback on the efficacy of your cybersecurity program.

You may not be able to answer all these questions on your own, so it is important to know who carries out cybersecurity activities at your organization and to communicate with them.

HOW TO STRUCTURE YOUR INFORMATION SECURITY PROGRAM

Your information security program will be shaped by your organization's unique needs and business processes. There is no one-size-fits-all solution. The Cybersecurity Framework (CSF), published by the National Institute for Standards and Technology (NIST), is a flexible, adaptable tool for organizing any information security program, regardless of size and resources. Although an institution will never be completely invulnerable, organizing your bank or non-bank cybersecurity program around the NIST CSF supports a comprehensive level of risk management.

The Framework organizes cybersecurity into five core "Functions," each of which represents a collection of behaviors: Identify, Protect, Detect, Respond, and Recover.

FIGURE 1: NIST Cybersecurity Framework Functions

IDENTIFY
internal and external risks.

PROTECT
organizational systems, assets, and data.

DETECT
active threats to your systems, including intrusions, data breaches, and unauthorized access

RESPOND
to cybersecurity events

RECOVER
and restore normal operations and services

Please note the Federal Financial Institutions Examination Council (FFIEC) provides a mapping of the FFIEC Cybersecurity Assessment Tool (CAT) to the NIST CSF for ease of coordination and communication. Find out more at https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_B_Map_to_NIST_CSF_June_2015_PDF4.pdf.

IDENTIFY

The Identify function helps establish what your organization must protect. Identify activities include determining what assets—both physical and informational—are present within your institution; how they fit in within the business environment; and the governance in place to manage your organization's regulatory, legal, and operational environments.

All of these activities make up your **risk assessment**, an evaluation of the threats faced by your institution, the likelihood they will happen, and the magnitude of harm should they occur. The results of your risk assessment will influence the overall risk management strategy, or how you plan to conduct business operations in such a way to limit risk to an acceptable level.

A risk assessment should be performed at least annually to confirm if an organization's resources, priorities, or business operations have changed significantly enough to warrant a strategy modification.

A cybersecurity risk assessment should classify critical information assets, identify threats and vulnerabilities, and communicate that risk to necessary personnel, including the Board. Before you can adequately assess risk to your institution, though, you must first identify your **Crown Jewels**, or your most critical information assets. "Crown jewels" are often highly sensitive and guarded and their loss, destruction, or theft could severely impact your institution.

IDENTIFYING THREATS

To identify potential cybersecurity threats, your financial institution may use internal resources, such as audit reports, vulnerability scans, and fraud detection tools; or external resources, such as information sharing networks like the **Financial Services – Information Sharing and Analysis Center (FS-ISAC)** and the **United States Computer Emergency Readiness Team (US-CERT)**. A tool like a vulnerability scanner is also commonly used to identify weaknesses by scanning your business environment against well-known and previously identified vulnerabilities. You can also test to determine if an identified vulnerability is actually exploitable.

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

FS-ISAC FOR FINANCIAL INSTITUTIONS

FS-ISAC offers a basic membership for community banks with less than $1 billion in assets which includes the "must-have" services shown below. Non-banks can also obtain FS-ISAC membership. 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 only provides notification of public urgent and crisis alerts. Learn more at https://www.fsisac.com/join.

FS-ISAC'S SERVICES FOR COMMUNITY BANKS:

- FS-ISAC established the Community Institution Council (CIC) to provide a forum for community banks to share information. All new community banks/credit union members are added to this group.
- FS-ISAC distributes weekly Risk Summary Reports to all community bank members. These reports help explain how the latest risks affect banks and their customers, and how these risks can be mitigated.
- Community Bank FS-ISAC members have access to the FS-ISAC Security Tool Kit, a 72-page document developed collaboratively with community institutions designed to provide a set of security practices to help strengthen banks' information security programs in light of increasing threats.
- FS-ISAC disseminates actionable threat, vulnerability and incident data to all members.

Data Breach Investigations Report and *Symantec's Internet Security Threat Report*. Both reports are updated annually.

Threat identification should occur continuously throughout the year and not only during the annual risk assessment. When news of a fraud, breach, or other incident emerges, consider whether your organization is also vulnerable. Could the same thing happen to your institution? What controls are in place to help protect against the threat?

MEASURING RISK

To effectively measure your organization's level of risk, a method for measuring risk must be developed. One approach is to give each asset a value of high, medium, or low. The rating can be financial but should also factor in how critical the asset is to your business. The risk level of those information assets is also given a rating of high, medium, or low. The final level of risk depends on remediation actions taken by your institution; mitigating controls can reduce the overall level of risk. For example, if backups are routinely performed, the risk posed by the loss of an electronic file may be low.

COMMUNICATING RISK

It is vital to establish a process that informs senior management and the Board of Directors about cyber risks to your organization, how your organization currently manages and mitigates those risks, and who is accountable for doing so. Once the risk assessment is developed, adopted, and approved, it should be reviewed and updated at least annually, or when changes to the environment are made, to ensure new risks are identified.

The risk assessment is one element of a larger cyber risk management process that each organization should have in place. CEOs should strive to create and implement an effective and resilient risk-management process that enables proper oversight and ensures effective management of cybersecurity risk. Key elements of a risk management process 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.

INFORMATION SECURITY TRIAD

Confidentiality, Integrity, and Availability (CIA) form the **information security triad**. Information security programs should be set up to ensure the CIA of all information assets, from data to hardware to networks.

- **Confidentiality** means information is protected from unauthorized access or disclosure.
- **Integrity** confirms information is trustworthy, accurate, and protected from unauthorized modifications.
- **Availability** guarantees reliable access to and use of information and information systems.

KEY "IDENTIFY" POINTS

IDENTIFY THE KEY PERSONNEL

responsible for your information security program.

DETERMINE YOUR ORGANIZATION'S RISK TOLERANCE

by assessing business priorities and regulatory and legal requirements.

IDENTIFY AND DOCUMENT

your assets. Know what you have, what it is used for, and to whom it belongs. Your most critical assets require the most protection.

DETERMINE THE BIGGEST THREATS

facing your organization. These could be physical, natural, or technology-based.

ESTABLISH GOVERNANCE,

including operating procedures and the identification of key personnel, to guide your information security program.

ACTIVELY MANAGE AND REPORT

the status of remediation plans to the Board.

REEVALUATE YOUR RISK TOLERANCE

and risk management strategy at least annually.

ESTABLISH A FREQUENCY

with which the Board will be updated on your organization's cybersecurity stature.

PROTECT

Once institutional threats are identified, the next step is to ensure your financial institution has safeguards commensurate with your risk profile. The Protect function includes establishing physical and information security controls, employee training programs, and operational processes that work to ensure your information and assets remain safe. Protection activities can be physical, such as behavioral processes, or technical, like automated tools.

Incorporate cybersecurity into your human resources and IT acquisition processes. Planning ahead reduces the likelihood of a catastrophic event occurring, as well as associated mitigation costs. Do not store all crown jewels in one place and ensure backup copies of data are stored in a secure, separate location. For more information on information and business recovery planning, as well as to explore backup agreements with other institutions, please visit Sheltered Harbor at https://shelteredharbor.org.

Malicious actors often gain access to valuable resources due to avoidable human error, so ensure your employee training program includes cybersecurity best practices and social engineering exercises. All attempts should be made to enact the same safeguards and protections at all work locations, including telework and remote locations. Your protection processes should be regularly updated, whenever your business environment changes or if a vendor informs you of an identified weakness. Test the effectiveness of protection tools and processes, whether by internal audits and scanning and/or by engaging the services of a penetration tester.

Another common threat vector is less secured vendors that are given access to your systems. Vendor management should include security reviews of vendors with system access and specify contractual requirements that vendors protect your information at least as well as you do.

SHELTERED HARBOR: RECOVERY OF LAST RESORT

Sheltered Harbor is an organization dedicated to protecting financial information from permanent loss through the establishment of best practices and a secure backup program for critical institutional customer account data. In the event of a cyber-attack, Sheltered Harbor can transmit a victim institution's critical data to a partner organization, who will temporarily resume critical financial services until the original provider's functions are restored.

FIGURE 2: CIS Top 20 Controls

The Center for Internet Security (CIS) publishes an annual list of the 20 controls most vital to a robust cybersecurity program. Institutions that effectively incorporate these controls are taking important steps to protect themselves and their consumers. CIS also makes available a Controls Self-Assessment Tool (CSAT) to help institutions determine how effectively the controls are applied. Learn more at https://www.cisecurity.org/cybersecurity-tools.

BASIC CIS CONTROLS

1| Inventory and Control of Hardware Assets
2| Inventory and Control of Software Assets
3| Continuous Vulnerability Management
4| Controlled Use of Administrative Privileges
5| Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6| Maintenance, Monitoring and Analysis of Audit Logs

FOUNDATIONAL CIS CONTROLS

7| Email and Web Browser Protections
8| Malware Defenses
9| Limitation and Control of Network Ports, Protocols and Services
10| Data Recovery Capabilities
11| Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12| Boundary Defense
13| Data Protection
14| Controlled Access Based on the Need to Know
15| Wireless Access Control
16| Account Monitoring and Control

ORGANIZATIONAL CIS CONTROLS

17| Implement a Security Awareness and Training Program
18| Application Software Security
19| Incident Response and Management
20| Penetration Tests and Red Team Exercises

CYBERSECURITY STAFF TRAINING RESOURCES

Start a conversation! The Federal Deposit Insurance Corporation's (FDIC) "Cyber Challenge" encourages community banks to run through and practice their responses to hypothetical cyber scenarios. Find it at: https://www.fdic.gov/regulations/resources/director/technical/cyber/cyber.html.

The National Cyber Security Alliance (NCSA) website covers safety basics at: https://www.staysafeonline.org.

Check the security of your devices using free tools, made available by the NCSA at: https://staysafeonline.org/stay-safe-online/free-online-security-checkups-tools.

Use National Cybersecurity Awareness Month every October to reemphasize your organization's commitment to proper cyber hygiene. Details available at: https://www.dhs.gov/national-cyber-security-awareness-month.

The Small Business Association (SBA) provides a free training course on cybersecurity for small businesses. It can be accessed at: https://www.sba.gov/course/cybersecurity-small-businesses.

CYBERSECURITY AND HUMAN RESOURCES

It is vital to include cybersecurity in your human resources processes.

New hires should learn their data protection responsibilities on day one.

Maintain and review records of which employees are permitted to access sensitive information.

Track who possesses what assets, like computers, telephones, and printers, and have a plan to collect them from departing employees.

Create a notification process so the IT department knows to modify, restrict, or delete access when an employee is hired, transferred, out of the office for an extended period of time, or fired.

IT IS VITAL TO INCLUDE CYBERSECURITY IN YOUR HUMAN RESOURCES PROCESSES.

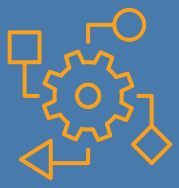
USEFUL PROTECTION TOOLS

- **Vulnerability Scanners** assess your environment for known vulnerabilities. Many are available for purchase; there are also free tools available online.
- **Security Information and Event Management** (SIEM) tools log and register activities performed on your systems.
- **Intrusion Detection Systems/ Intrusion Prevention Systems** (IDS/ IPS) alert your IT Team to potential intrusions. Some may even prevent attacks from successfully occurring.

KEY "PROTECT" POINTS

MAKE SURE PERSONNEL

in IT and information security can answer your questions about how data is protected.



ENSURE THE RESOURCES ARE ALLOCATED

for data protection are sufficient.

CREATE A PLAN

to collect IT resources and information from departing or transferred employees.

DETECT

Hackers will exploit any vulnerability they can find, and it's up to your IT staff information security staff, and employees to detect such intrusions. To effectively do this, you must first have a thorough understanding of what is in your asset inventory (see IDENTIFY Section) and how assets are protected (see PROTECT Section).

Your IT and information security staff can then monitor and assess normal business behaviors and look for anomalies. The process is called continuous monitoring, which just means at any point your staff can know what is occurring on your network.

A few common ways to detect intrusions are by using automated tools, like an intrusion detection system (IDS), malware detection tools, data loss prevention tools (DLP) and big data analytics. Other detection methods include independently reviewing records of who accessed what information or facility and following up on anomalies reported by internal users. Engaging the services of a penetration tester, a hacker who tries to gain access to your system (with your advance knowledge) by exploiting unknown vulnerabilities, will also help you determine possible system access points for intruders.

KEY "DETECT" POINTS

MAKE SURE YOUR EMPLOYEES KNOW WHAT TO LOOK FOR.

Set a baseline of normal behaviors so anomalies can be detected.

CONFIRM YOUR THIRD-PARTY VENDORS

actively scan for anomalous behavior and notify you.

TEST YOUR ORGANIZATION'S ABILITY

to detect events at least annually.

RESPOND

Detecting an incident is less useful if your organization does not know how to respond. An incident response plan is an organized approach to addressing and managing a security breach or attack. The incident response plan should include a policy that defines what constitutes an incident, and it should provide a step-by-step process that should be followed when an incident occurs.

An incident response plan will help your institution successfully understand, manage, and recover from a cyber-attack. Without it, an organization may not even discover an attack in the first place; or, if the attack is discovered, the institution may not follow good procedures to contain damage, eradicate the attacker's presence, or recover in a secure fashion.

An incident response plan should address:

- The official incident response team, or personnel with response obligations (often includes high-level executives and the CEO, legal representation, information security and IT personnel, and public relations and communications experts);
- Scenarios your organization considers worthy of investigation and the threshold for declaring an incident;
- The chain of command, including who has the authority to declare an official incident; and
- The severity levels that an incident may be sorted (usually low, moderate, or high).

BREACH NOTIFICATION

Reporting requirements vary state-by-state and may include federal and international laws in addition to state laws. Please refer to your applicable breach notification law(s), which are available at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

INCIDENT RESPONSE GUIDE

A comprehensive guide on forming and executing an incident response plan is available from NIST at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

An incident response plan should include:

- Steps that may be taken to address potential damage and to limit the loss of resources, including any required timelines or Service Level Agreements (SLAs);
- Contractual or regulatory reporting requirements;
- Projected time and resources required to implement the response strategy; and
- A communications plan that incorporates:
  - when and if you should report a breach to the media and/or notify affected individuals;
  - the preferred medium for notification;
  - basic guidelines for tracking and analyzing media coverage; and
  - a process for notifying employees of the incident and instructing them about immediate containment steps.

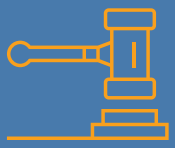
For incident response best practices information on how to form and execute a plan, please refer to:

- NIST Computer Security Incident Handling Guide at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.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.

"UNDERSTANDING THREATS AND IDENTIFYING MODERN ATTACKS IN THEIR EARLY STAGES IS KEY TO PREVENTING SUBSEQUENT COMPROMISES [...]"

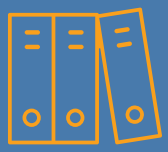
– NIST Computer Security Incident Handling Guide

KEY "RESPOND" POINTS



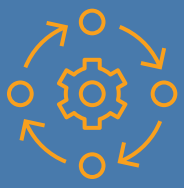
ESTABLISH LEGAL REPRESENTATION AHEAD OF TIME.

Breach counsel will help your organization navigate response activities, liabilities, and legalities, all while maintaining attorney-client privilege.



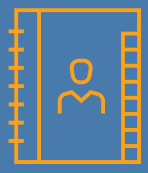
KNOW YOUR LEGAL AND CONTRACTUAL REPORTING RESPONSIBILITIES.

Determine if any internal, external, or agency stakeholders must be notified within a specified timeframe.



PRACTICE MAKES PERFECT!

Run through your incident response plan at least annually with all team personnel. Adjust your plan for different types of cyber incidents.



ESTABLISH AND MAINTAIN KEY LAW ENFORCEMENT POINTS OF CONTACT,

including local police, the Federal Bureau of Investigation (FBI), and the United States Secret Service (USSS).

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.

RECOVER

After your institution has taken steps to respond to a cyber incident, the next step is the Recover phase.

Recovery includes public relations activities undertaken to mitigate reputational risk, the resolution of internal and stakeholder communications, and the updating of your recovery plans with lessons learned.

By the end of the recovery period, your infrastructure, data, and services should all be restored. This may take anywhere from hours to weeks, but with proper planning it should occur within the predicted timeline.

KEY "RECOVER" POINTS

MAKE SURE YOU HAVE A PLAN

to restore all business operations, including a communications plan.

CONFIRM

that each of your third-party vendors maintains its own recovery plan.

TAKE STEPS TO MITIGATE

reputational risk resulting from the incident.

TAKE NOTES ABOUT WHAT WORKED

and what didn't so you can update your recovery plan.

Glossary

Crown Jewels – An organization's most critical information assets

Cybersecurity – The ability to protect or defend the use of cyberspace from cyberattacks

Denial of Service – An attempt to overwhelm a website or tool with requests so it becomes useless

Information Availability – Information and information systems are accessible and reliable

Information Confidentiality – Information is protected from unauthorized access or disclosure

Information Integrity – Information is trustworthy, accurate, and protected from unauthorized modifications

Insider Threat – A threat posed by employees, vendors, and people close to the business, either on purpose or by accident

Phishing – An attempt to prey on a user's sense of responsibility, empathy, or urgency to trick him or her into sharing credentials with an unauthorized user

Ransomware – An attack that encrypts valuable computer resources and holds them hostage until a ransom is paid

Risk – The likelihood and potential magnitude of harm

Risk Assessment – An evaluation of the threats faced by an institution, the likelihood they will happen, and the magnitude of harm should they occur

Threat – A force, organization, or person with the potential to obtain, compromise, or destroy an information asset

Vulnerability — A weakness

BY THE END OF THE RECOVERY PERIOD, YOUR INFRASTRUCTURE, DATA, AND SERVICES SHOULD ALL BE RESTORED.

Resources

DISASTER RECOVERY

Sheltered Harbor
https://www.shelteredharbor.org/

FRAMEWORKS

The Center for Internet Security's (CIS) 20 Critical Security Controls
https://www.cisecurity.org

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)
https://www.nist.gov/cyberframework

INFORMATION SHARING

The Center for Internet Security (CIS) Controls Self-Assessment Tool (CSAT)
https://www.cisecurity.org/blog/cis-csat-free-tool-assessing-implementation-of-cis-controls/

The Financial Services Information Sharing and Analysis Center (FS-ISAC)
https://www.fsisac.com/about

Federal Financial Institutions Examination Council (FFIEC)
https://www.ffiec.gov/about.htm

The National Cybersecurity Alliance
https://staysafeonline.org/

Symantec 2019 Internet Security Threat Report 2019
https://www.symantec.com/security-center/threat-report

United States Computer Emergency Readiness Team (US-CERT)
https://www.us-cert.gov/

United States Department of Homeland Security (DHS) Stop. Think. Connect™
https://www.dhs.gov/stopthinkconnect

Verizon 2019 Data Breach Investigations Report
https://enterprise.verizon.com/resources/reports/dbir/2019/introduction/

PENETRATION TESTING

Department of Homeland Security – Free
https://krebsonsecurity.com/2015/12/dhs-giving-firms-free-penetration-tests/

THE CONFERENCE OF STATE BANK SUPERVISORS
www.csbs.org / @csbsnews