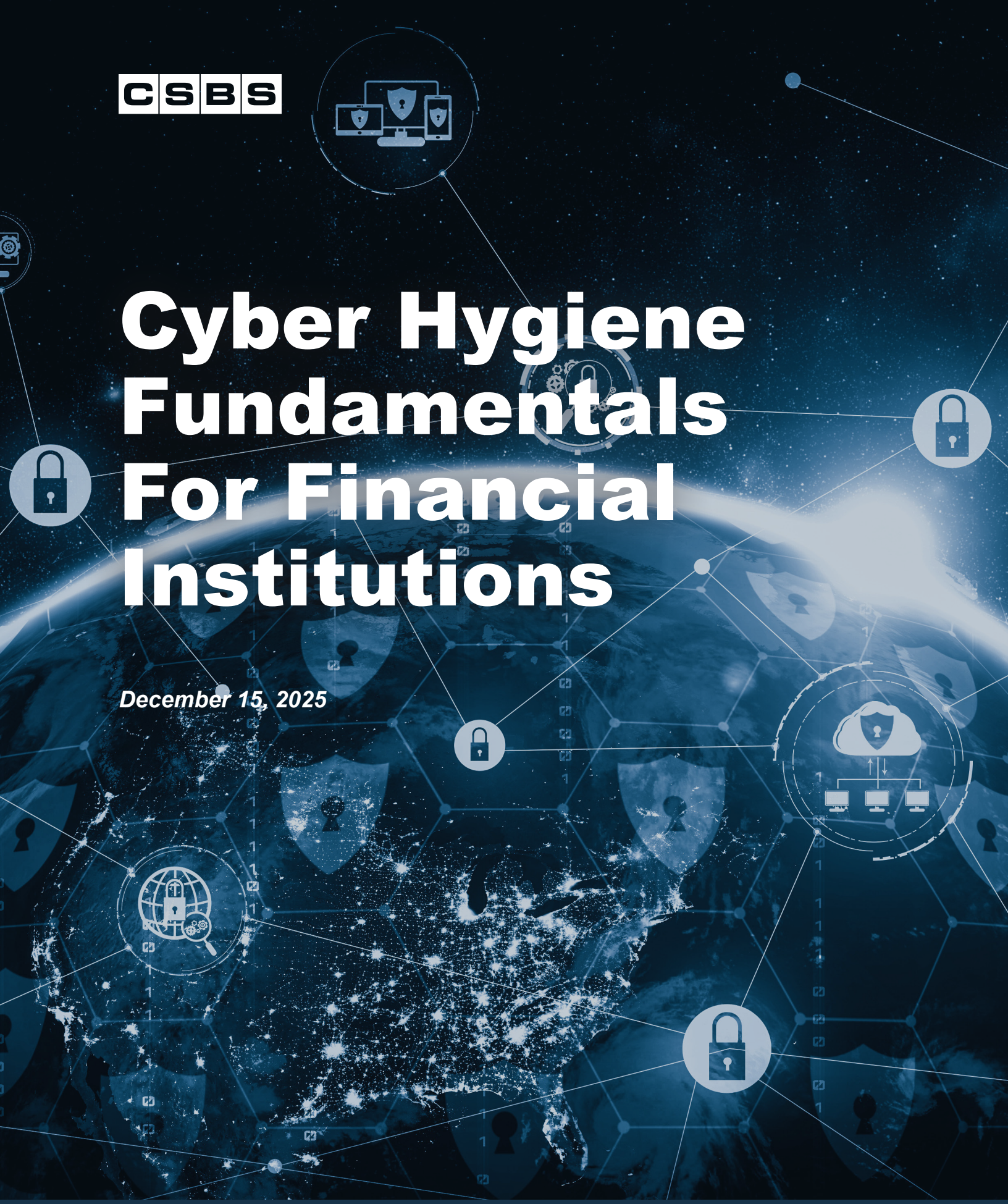


Cyber Hygiene Fundamentals For Financial Institutions

December 15, 2025

CYBERSECURITY AWARENESS TRAINING

Why is cybersecurity awareness training important?

Cybersecurity awareness training for bank employees is critically important because banks are prime targets for cyberattacks due to the sensitive financial data they handle. Proper training programs are the foundation for a ***sound culture of cyber awareness throughout the institution*** and can help counter inherent weaknesses in human interaction with computers and data. Human error has been cited as a contributing factor in 95% of all cyber incidents that occurred in 2024.[3] Training helps to strengthen the overall quality of our defenses against cyber threats.

Cybersecurity awareness training basics

Effective cybersecurity awareness training programs should be available for all employees and possess the following characteristics:

- **Appropriate frequency;**
- **Simulated exercises;**
- **A dynamic curriculum to address both existing and emerging threats; and**
- **Out-of-cycle training.**

Appropriate frequency: how often should training be offered?

Annual cybersecurity training has long been viewed as a minimum frequency standard in financial institutions. However, while annual training programs may be suitable for some institutions, there is growing evidence that more frequent cyber awareness training can be more effective. In fact, organizations such as ISACA recommend training every four to six months to ensure that individuals more effectively retain the ability to apply what they have learned.[4] Institutions are encouraged to holistically examine the scope and track record of their cybersecurity training programs to determine the most appropriate frequency for delivery of employee awareness training.

Simulated exercises

A continuous program of ***phishing exercises*** can provide multiple benefits to the institution and its employees. While not a substitute for regular, full-scope cybersecurity training, periodically exposing all employees to random, simulated phishing emails more closely mimics what they see in real-world interactions and helps to both train and measure their ability to spot phony email messages, malicious attachments, and harmful links. This is particularly important given the growing sophistication and effectiveness of phishing techniques, such as AI-enhanced phishing, used by modern threat actors. Phishing exercises also provide trackable real-time metrics of employee awareness to institution management, such as *open rate, click rate, and report rate*, which can guide future training efforts and help to identify areas where immediate refresher emphasis might be needed.[5]

Employee training curriculum

There are three areas to consider for an employee awareness training curriculum:

- ***Existing and emerging threats to the institution***. Employees should be aware of the general threat landscape and the general nature of threat actor tactics, indicators and red flags, etc. Specific training topics should ideally address existing threats, as well as emerging threats to the institution. For example, many training programs today address existing threats such as ransomware, phishing, insider threats, and social engineering. However, with the recent emergence of artificial intelligence and the use of deep fakes by cyber threat actors, it is now most practical to also consider these and other emerging areas when planning the training curriculum.
- ***Incident identification and reporting mechanisms***. If an employee observes suspicious activity or inadvertently engages with a malicious email, file, or link, they should be aware of the appropriate procedures for reporting such encounters to management or IT security teams. Moreover, they should feel no hesitation or fear of reprisal in reporting such encounters, regardless of whether they are suspected or actual incidents. Incidents do happen, and management should feel confident, through its training program, that employees will be willing and capable of following established reporting protocols when they do occur.
- ***Acceptable use policy training and employee acknowledgement***. According to the FFIEC, "Training should support security awareness and strengthen compliance with security and acceptable use policies."[6] In most institutions, the acceptable use policy provides specific guidance regarding expectations for employee interactions with company systems. This policy generally addresses considerations such as web browsing, email usage standards, and social media guidelines. Formal training should include curricula addressing the expectations specific to the institution's acceptable use policy. Moreover, to reduce confusion and foster employee compliance, a written attestation should ideally be obtained annually for every employee interacting with company systems (including senior and executive management) acknowledging that the policy has been read, and its requirements are understood. [7]

The institution should also implement a dynamic program to ***track employee compliance with training requirements***. Management should frequently compare completed training assignment records and required due dates, and a process for follow-up, including escalation procedures for noncompliance, should be in place to ensure the completeness of training efforts. Finally, because senior leadership within the institution is frequently targeted by cyber threat actors, training program requirements and tracking should extend to all individuals who are granted access to company data or systems, regardless of their position in the institution's hierarchy. This would also include any board members with institution email addresses or access to institution networks or systems.

Out-of-cycle training

Due to the dynamic nature of the cyber threat environment, it is often necessary to **provide employees with timely, meaningful information concerning emerging risks in between established training cycles.** Institutions should consider the development of a mechanism to inform employees of relevant threats on an ongoing basis. This can be accomplished through the delivery of threat information via awareness emails from IT security personnel or during branch or department meetings.[8]

> ***...provide employees with timely, meaningful information concerning emerging risks in between established training cycles.***

A strong cyber awareness culture is critical to long-term success

A strong employee awareness training program is a key component necessary to establish an ***ongoing culture of cyber awareness in the institution***. The constantly evolving and extremely dangerous nature of today's threat landscape requires a dynamic approach to maintaining employee awareness of these threats. Institutions must empower employees to react to this changing landscape through recognition and reporting of these threats when they arise. Institutions that transform their training programs from one-off, perfunctory exercises into meaningful, dynamic programs will enjoy greater success in repelling existing and emerging threats and increasing protections for customer data and institution systems.

> ***A strong employee awareness training program is a key component necessary to establish an ongoing culture of cyber awareness in the institution.***

Below are some questions you may ask management to ensure that the institution's cybersecurity awareness training program is sufficient to develop and maintain appropriate employee knowledge of ongoing and emerging threats against the institution.

1 How frequently does the institution conduct formal cybersecurity awareness training for all employees, including senior management and executives?

WHY THIS IS IMPORTANT: While annual training programs may be suitable for some institutions, there is growing evidence that more frequent cyber awareness training can be more effective. Organizations such as ISACA recommend training every four to six months to ensure that individuals more effectively retain the ability to apply what they have learned.[9] Institutions are encouraged to holistically examine the scope and track record of their cybersecurity training programs to determine the most appropriate frequency for delivery of employee awareness training. Training program requirements and tracking should extend to all individuals who are granted access to company data or systems, regardless of their position in the institution's hierarchy. This would also include any board members with institution email addresses or access to institution networks or systems.

2 Is there a program to track employee completion of assigned cybersecurity awareness training?

WHY THIS IS IMPORTANT: The institution should also implement a dynamic program to track employee compliance with training requirements. Management should frequently compare completed training assignment records and required due dates, and a process for follow-up, including escalation procedures for noncompliance, should be in place to ensure the completeness of training efforts for all employees.

3 Does the institution conduct phishing training to expose employees to simulate real-world threats?

WHY THIS IS IMPORTANT: While not a substitute for regular, full-scope cybersecurity training, periodically exposing all employees to random, simulated phishing emails more closely mimics what they see in daily real-world interactions and helps to both train and measure their ability to spot phony email messages, malicious attachments, and harmful links. This is particularly important given the growing sophistication and effectiveness of phishing techniques, such as AI-enhanced phishing, used by modern threat actors. Phishing exercises also provide trackable real-time metrics of employee awareness to institution management, which can guide future training efforts and help to identify areas where immediate refresher emphasis might be needed.[10]

4 Does the institution's training curriculum address:

a. **Existing and emerging threats to the institution**

b. **Incident identification and reporting mechanisms**

c. **Acceptable use policy training and employee acknowledgement?**

WHY THIS IS IMPORTANT: Employees should be aware of the general threat landscape and the general nature of threat actor tactics, indicators and red flags, etc. While many training programs today address existing threats such as ransomware, phishing, insider threats, and social engineering, the recent emergence of artificial intelligence and the use of deep fakes by cyber threat actors, it is now most practical to consider these and other emerging areas when planning the training curriculum.

If an employee observes suspicious activity or inadvertently engages with a malicious email, file, or link, they should be keenly aware of the appropriate procedures for reporting such encounters to management or IT security teams. Moreover, they should feel no hesitation or fear of reprisal in reporting such encounters, regardless of whether they are suspected or actual incidents.

Formal training should include curricula addressing the expectations specific to the institution's acceptable use policy. A written attestation should ideally be obtained annually for every employee interacting with company systems (including senior and executive management) acknowledging that the policy has been read and its requirements are understood. [11]

5 Does the institution regularly expose employees to meaningful threat information, as appropriate, between formal training cycles?

WHY THIS IS IMPORTANT: Due to the dynamic nature of the cyber threat environment, it is often necessary to provide employees with timely, meaningful information concerning emerging risks in between established training cycles. This can be accomplished through the regular delivery of threat information via awareness emails from IT security personnel or during branch or department meetings.[12]

DATA BACKUP PROGRAMS

Why are data backup programs important?

Ransomware attacks, data corruption events, and hardware failure can quickly render mission-critical data inaccessible or unusable—potentially producing immediate and devastating consequences for the affected institution. A robust data backup program ensures that critical business systems and data, including core processing, network administration, and customer records, can be recovered when these events occur. These programs are the backbone of an institution's ability to restore services and maintain operational continuity.

Effective backup programs go beyond simply saving files—they must also include protections against ransomware, test restorability, and allow for off-network restoration if the primary environment is compromised.

Data backup program basics

According to the FFIEC, decisions to implement any particular methodology for backing up data, including the use of replication, should be "based on the risk and criticality of the systems and data."[13] The CSBS Ransomware Self-Assessment Tool (R-SAT) outlines eight key control considerations for implementing and maintaining an effective data backup program. These control considerations are applicable for core processing, network administration, and other data driven critical services, such as trust services, mortgage loans, investments, image files, email services, etc.

- **Ransomware and extortion-resilient procedures**: Ensure that backup procedures include isolation, segmentation, and protections to protect malware from accessing or encrypting backup data files. This may involve utilization of immutable (unalterable) storage methods, air-gapping techniques, and endpoint protections on backup architecture.
- **Distinct authentication methods for access to backups**: Restrict access to backup environments using unique login credentials that are separate from those used for access to the primary network. This can assist in creating an audit trail and can help limit threat actor access when stolen network user or administrative credentials are used to gain access during an attack.
- **Daily full system backups**: Full system backups (not just incremental backups) should ideally be performed at least daily. This procedure helps to ensure that a complete, reliable copy of the data environment is always available. If full data backups are not feasible, the institution should categorize its data by criticality, decide the nature of data to be included, and determine the appropriate frequency of backups to ensure that current, critical data is available when needed.

- **Redundant media types to store backups:** Ideally, institutions will maintain at least two copies of backups stored on different media types (i.e., disk, cloud, flash drive, etc.) and, most ideally, hold them in separate, secure locations. This will help to ensure accessibility in the event of failure of the mechanism(s) utilized to access, read, and restore backup data.
- **Offline or immutable backups**: Ensure that at least one backup is held offline in an air-gapped environment or in an immutable format. According to IBM, "*Air gapping* refers to the physical separation of computers and networks, while *air-gapped networks* are networks that have been isolated from all external networks, including cloud and wi-fi. Air-gapped networks are disconnected from the internet and provide a strong layer of protection from a broad range of cybersecurity threats."[14]
- **Off-network restoration capabilities:** Establish procedures for immediate restoration of backups in a separate, off-network environment in the event primary systems are locked down or otherwise unavailable.
- **Annual backup testing:** Data backup systems should ideally be tested at least annually to confirm that successful data restoration can be reliably performed. Backup testing can be accomplished as a stand-alone process or it may be incorporated into the institution's larger business continuity or incident response testing exercises. Backup tests should be documented, and any identified deficiencies should be remediated.
- **Validation of backup sterility:** Before restoration, verify that backups are free from malware to prevent possible cross-contamination and reinfection. This includes scanning backups before use and verifying the integrity of the backup data.

Other data backup program considerations

Reassess backup and recovery strategies

According to the FFIEC, backup and recovery strategies should be reassessed as technology and threat environments evolve. More advanced duplication and backup methods may be appropriate for real-time or high-volume systems. These advanced methods, including cloud and mirroring, provide high data availability to the institution. Moreover, "Management should maintain an accessible, off-site repository of software, configuration settings, and related documentation. Even standard software configurations can vary from one location to another. Differences could include parameter settings and modifications, security profiles, reporting options, account information, customized software changes, or other options. Failure to back up software configurations could result in inoperability or could delay recovery."[15]

Determine appropriate data retention periods

Appropriate retention periods should be determined for each iteration of data backup. Protections should be in place to prevent the replication of malware and data corruption, the risk of which is enhanced with the use of near real-time data replication systems, as malware can be replicated undetected. According to the FFIEC, "Even with diagnostic tools, management could be unaware of an event that causes data integrity issues until well after it happens, as data could appear uncorrupted but later determined to be inaccurate. Management may determine that the backup of critical data files should be subject to longer retention periods to ensure the ability to recover a backup prior to a corruption event."[16]

Develop appropriate cyber resilience processes

Finally, the FFIEC notes that, "Entities should develop **appropriate cyber resilience processes** (e.g., recovery of data and business operations, rebuilding network capabilities and restoring data) that enable restoration of critical services if the institution or its critical service providers fall victim to a destructive cyberattack or similar event. Business continuity management (BCM) should include the ability to protect offline data backups from destructive malware or other threats that may corrupt production and online backup versions of data."[17] Institutions that rely on third-party service providers, including cloud service providers, to manage their backup and replication processes should validate and ensure the provider maintains satisfactory processes that address, among other considerations, inventories of backup media; processes for testing backups; capabilities to restore to a previous trusted state; protections against malware, destruction, and corruption; and policies, procedures, and standards that document methodologies, prescribe personnel responsibilities, and promote consistent performance.[18]

Below are some questions you may ask management to ensure that the institution's data backup program is sufficient to allow the institution to restore critical business systems and data in the event of a ransomware attack, data corruption event, or hardware failure.

1 Explain the controls our institution has in place for data backups.

WHY THIS IS IMPORTANT: Backup procedures **include isolation, segmentation, and protections** to protect malware from accessing or encrypting backup data files. This may involve utilization of immutable (unalterable) storage methods, air-gapping techniques, and endpoint protections on backup architecture.

Access to backup environments should be restricted using unique login credentials that are separate from those used for access to the primary network. This can assist in creating an audit trail and can help limit threat actor access when stolen network user or administrative credentials are used to gain access during an attack.

Full system backups (not just incremental backups) should ideally be performed at least daily. This procedure helps to ensure that a complete, reliable copy of the data environment is always available. If full data backups are not feasible, the institution should categorize its data by criticality, decide the nature of data to be included, and determine the appropriate frequency of backups to ensure that current, critical data is available when needed.

Ideally, institutions will **maintain at least two copies of backups stored on different media types** (i.e., disk, cloud, flash drive, etc.) and, most ideally, hold them in separate, secure locations. This will help to ensure accessibility in the event of failure of the mechanism(s) utilized to access, read, and restore backup data.

Ideally, **at least one backup should be held offline in an air-gapped environment or in an immutable format**. According to IBM, "Air-gapped networks are disconnected from the internet and provide a strong layer of protection from a broad range of cybersecurity threats."[19]

Procedures should be established for **immediate restoration of backups in a separate, off-network environment** in the event primary systems are locked down or otherwise unavailable.

Data backup systems should ideally be tested at least annually to confirm that successful data restoration can be reliably performed. Backup tests should be documented, and any identified deficiencies should be remediated immediately.

Before restoration, the institution should **verify that backups are free from malware** to prevent possible cross-contamination and reinfection. This includes scanning backups before use and verifying the integrity of the backup data.

2 Does management periodically reassess the institution's data backup strategy?

WHY THIS IS IMPORTANT: According to the FFIEC, **backup and recovery strategies should be reassessed as technology and threat environments evolve**. More advanced duplication and backup methods may be appropriate for real-time or high-volume systems. These advanced methods, including cloud and mirroring, provide high data availability to the institution. Moreover, "Management should maintain an accessible, off-site repository of software, configuration settings, and related documentation. Failure to back up software configurations could result in inoperability or could delay recovery."[20]

3 Does management consider data retention periods for each iteration of data backup?

WHY THIS IS IMPORTANT: Appropriate retention periods should be determined for each iteration of data backup. Protections should be in place to prevent the replication of malware and data corruption, the risk of which is enhanced with the use of near real-time data replication systems, as malware can be replicated undetected. According to the FFIEC, "Even with diagnostic tools, management could be unaware of an event that causes data integrity issues until well after it happens, as data could appear uncorrupted but later determined to be inaccurate. Management may determine that the backup of critical data files should be subject to longer retention periods to ensure the ability to recover a backup prior to a corruption event."[21]

4 Does the institution maintain appropriate cyber resilience processes that enable the restoration of critical services if the institution or its critical service providers fall victim to a destructive cyberattack or similar event?

WHY THIS IS IMPORTANT: According to the FFIEC, "Business continuity management (BCM) should include the ability to protect offline data backups from destructive malware or other threats that may corrupt production and online backup versions of data."[22] Supporting processes should allow for the recovery of data and business operations, the rebuilding of network capabilities, and the restoration of data.

Institutions that rely on **third-party service providers**, including **cloud service providers**, to manage their backup and replication processes should validate and ensure the provider maintains satisfactory processes that address, among other considerations, inventories of backup media; processes for testing backups; capabilities to restore to a previous trusted state; protections against malware, destruction, and corruption; and policies, procedures, and standards that document methodologies, prescribe personnel responsibilities, and promote consistent performance.[23]

END-OF-LIFE (EOL) MANAGEMENT

What are end-of-life (EOL) assets?

End-of-life (EOL) assets are retired software or hardware assets that no longer receive updates or security patches from their vendors, making them attractive and frequently compromised targets for cyber criminals.

Why is EOL management important for the institution?

The modern financial institution is increasingly dependent on technology to perform a host of tasks, ranging from applications that enable the most mundane of daily operations to the core platform systems that are the very lifeblood of the institution's operations. Yet, as this beneficial technology has increasingly become integrated into our institutions, so has the need increased for effective **life cycle management of technology assets**. Institutions commonly maintain patch management programs to handle ongoing maintenance and updating of hardware and software assets. However, these same hardware and software assets generally have limited life spans and, because updates and security patches are generally not provided (without special arrangements) once these assets are retired by their vendors, they become attractive and frequently compromised points of entry for cyber criminals. For this reason, **it is vitally important that every institution maintains a program to identify and manage EOL assets and the associated risks as part of the larger asset life cycle management program.** The institution simply cannot manage or apply adequate security protections to assets it does not know it has.

Financial institutions often find comfort in the reliability and convenience of the technology tools that enable their everyday business operations. Moreover, financial considerations and the costs of implementing and integrating new technology can further increase disdain on moving away from outdated or unsupported technology. However, there are several important reasons why EOL management is so critical for financial institutions. Inadequate management of EOL hardware and software assets and relying on outdated or unsupported technology can create:

- **Exploitable vulnerabilities**. Unpatched or outdated technology opens the door to easily exploitable and frequently targeted vulnerabilities, which can lead to unauthorized access to information, data breaches, and the introduction of malware.
- **Compatibility issues**. Leaving EOL assets or outdated technology in the environment may lead to compatibility issues with other technologies in the institution. Future upgrades or replacements of other technologies may conflict with unsupported legacy hardware and software, creating conflicts, limiting modernization efforts or affecting usability and security of existing technologies.
- **Increased costs.** Unsupported technology can lead to Increased costs associated with maintaining outdated software, addressing usability conflicts, and potential reductions in system performance, security, or reliability.[24]

Clearly, the risks and potential costs of maintaining outdated and unsupported hardware and software assets far outweigh any benefits of relying on unsupported technologies. But getting a handle on the management of outdated hardware and software assets is an ongoing process that requires a clear view of all the institution's assets and an understanding of the interdependencies that exist between outdated assets and other institution systems.

Understanding the EOL management process

Management of EOL assets requires a forward-thinking approach, as replacing hardware and software assets generally requires awareness, time, and planning. This can create significant impacts on the operation of other systems in the institution and is rarely accomplished smoothly and without disruption in the absence of a comprehensive plan for replacement.

According to the FFIEC IT Handbook booklet: *Information Security*, "Management should plan for a system's life cycle, eventual end of life, and any corresponding security and business impacts. The institution's strategy should incorporate planned changes to systems, including an evaluation of the current environment to identify potential vulnerabilities, upgrade opportunities, or new defense layers." In addition, support from any third-party system vendors and the risks associated with operating unsupported legacy systems should be included in the institution's life cycle management strategy.[25] The FFIEC notes that effective EOL management should include the following:

- Maintaining inventories of systems and applications.
- Adhering to an approved end-of-life or sunset policy for older systems.
- Tracking changes made to the systems and applications, availability of updates, and the planned end of support by the vendor.
- Conducting risk assessments on systems and applications to help determine end-of-life.
- Planning for the replacement of systems nearing obsolescence and complying with policy requirements for implementing new systems or applications.
- Developing specific procedures for the secure destruction or data wiping of hard drives returned to vendors or donated, to prevent the inadvertent disclosure of sensitive information.[26]

Compensating controls

There may be instances where EOL systems must temporarily remain within the institution due to compatibility issues, special financial considerations, etc. In these cases, it is essential that compensating controls exist to mitigate the associated risk. These controls may include isolating or segregating the unsupported asset from the network, adjusting existing security configurations, and/or acquiring extended support and service contracts from the vendor, when available. According to the FFIEC, "Management should also have a plan to replace the system or application and implement compensating controls until replacement. Strategies for replacing and updating hardware and software should incorporate and align with overall information security and business strategies as appropriate."[27] Ongoing tracking of any unremediated EOL hardware or software assets can help ensure they are managed in accordance with the institution's risk acceptance policy and established risk tolerances prior to replacement.

Below are some questions you may ask management to ensure end-of-life (EOL) management practices has been appropriately implemented to protect against cyber threats.

1 Does the institution have processes in place to maintain a comprehensive and ongoing inventory of all hardware and software assets within the institution, including all assets that are not in regular use but may be deployed at any time on the institution's network?

WHY THIS IS IMPORTANT: Tracking all institutional hardware and software assets can be a daunting task, especially in larger institutions. However, it is vitally important that the institution have a process in place to identify and track assets to ensure they are included as part of the institution's ongoing vulnerability and patch management programs and, in the context of end-of-life management, that they are identifiable to afford the institution sufficient time to plan for their retirement by the vendor. The institution simply cannot manage or apply adequate security protections to assets it does not know it has.

2 Does the institution's asset identification process:

a. **Identify vendor-reported retirement or sunset dates for all hardware and software assets, and**
b. **Include the identification of asset interdependencies to avoid potential conflicts or operational issues once the asset is retired or replaced?**

WHY THIS IS IMPORTANT: Vendors typically announce the sunsetting of hardware and software assets with enough lead time to allow the institution to plan for their retirement, replacement, or the engagement of service contracts to support the asset past its sunset date. But simply identifying the asset's retirement date is likely not enough; proper end-of-life management ensures that plans for addressing a sunsetting asset also include the identification of any asset interdependencies and plans to address any potential operational issues with enough lead time to ensure that conflicts with other assets or processes are avoided to the extent possible.

3 Does the institution currently utilize any unsupported or out-of-date hardware or software assets? If so, are satisfactory compensating controls in place to reduce the risk associated with the continued use of these assets? Does the institution have an active plan to replace these unsupported or out-of-date assets?

WHY THIS IS IMPORTANT: Unpatched or outdated technology opens the door to easily exploitable and frequently targeted vulnerabilities. This can lead to unauthorized access to information, data breaches, and the introduction of malware. The continued use of end-of-life assets or outdated technology in the technology environment may also lead to compatibility issues with other technologies in the institution. Future upgrades or replacements of other technologies may conflict with unsupported legacy hardware and software, creating conflicts, limiting modernization efforts, or affecting usability and security of existing technologies. Finally, unsupported technology can lead to increased costs associated with maintaining outdated software, addressing usability conflicts, and potential reductions in system performance, security, or reliability.

4 Does the institution have a written policy in place to document the institution's end-of-life management strategy and processes, including:

a. **Replacing or retiring sunsetting assets and complying with institution requirements for implementing new systems or applications;**

b. **Identification of the risks of operating unsupported assets and guidance for implementing compensating controls for any assets that must be kept beyond their sunset date, including isolating or segregating the asset from the network, adjusting existing security configurations, and/or acquiring extended vendor service agreements, as necessary, to extend support for sunsetting assets;**

c. **Conducting risk assessments on systems and applications to identify potential vulnerabilities, upgrade opportunities, or new defense layers, and to help determine end-of-life; and**

d. **Specific procedures for the secure destruction or data wiping of hard drives returned to vendors or donated, to prevent the inadvertent disclosure of sensitive information?**

WHY THIS IS IMPORTANT: Management of end-of-life assets is a somewhat complex process that requires a forward looking, organized approach. A comprehensive end-of-life management policy provides structure for the institution's management of end-of-life assets, covering general asset identification and management strategies, as well as identification and management of the various risks associated with end-of-life assets.

INCIDENT RESPONSE PROGRAMS

Why are incident response programs important?

Financial institutions remain a prime target for cyber threat actors, primarily due to the wealth of personal and financial information they manage for their customers. The ability to quickly detect, contain, and recover from cyberattacks can help to lessen operational impacts and minimize the erosion of consumer trust, financial losses, and the regulatory consequences that can accompany a successful cyberattack. The institution's **incident response program** is the cornerstone that helps to ensure that these consequences are minimized to the greatest extent possible when a cyberattack occurs. Moreover, it is the key pillar of an institution's overall **resilience strategy** because it drives the institution's initial reactions to withstand and recover from disruptions that will inevitably occur.

Incident response basics

According to the FFIEC, "The goal of incident response is to minimize damage to the institution and its customers. The institution's program should have defined protocols to declare and respond to an identified incident. More specifically, the incident response program should include, as appropriate:

- Containing the incident;
- Coordinating with law enforcement and third parties;
- Restoring systems, preserving data and evidence;
- Providing assistance to customers; and
- Otherwise facilitating operational resilience of the institution."

Incident response "involves a combination of people and technologies" and that the quality of incident response is attributable to "the institution's culture and its policies, procedures, and training." In addition, it is "a function of the relationships the institution formed before the incident with law enforcement, incident response consultants and attorneys, information-sharing entities (e.g., FS-ISAC), and others." And at the heart of the incident response program is the **incident response plan (IRP)**. The IRP is the quintessential, living document that addresses the "action steps, involved resources, and communication strategy upon identification of a threat or potential event."[28]

To further illustrate the incident response life cycle, NIST has developed a "high-level incident response life cycle model based on the six CSF 2.0 Functions, which organize cybersecurity outcomes at their highest level:

- **Govern (GV)**: The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
- **Identify (ID)**: The organization's current cybersecurity risks are understood.
- **Protect (PR)**: Safeguards to manage the organization's cybersecurity risks are used.
- **Detect (DE)**: Possible cybersecurity attacks and compromises are found and analyzed.
- **Respond (RS)**: Actions regarding a detected cybersecurity incident are taken.
- **Recover (RC)**: Assets and operations affected by a cybersecurity incident are restored."[29]

Components of incident response

There are many considerations for financial institutions in developing and implementing an incident response program and incident response plan. The FFIEC highlights a number of **primary considerations**, including:

- Defining **policies and procedures** to guide responses to incidents
- Selecting, installing, and understanding the **tools that will play a part in the response process**
- Balancing **concerns regarding confidentiality, integrity, and availability for devices and data** (i.e., containment and restoration strategies which account for systems that can be disconnected and systems that must remain operational)
- Defining **circumstances when incident response activities are to be initiated**
- Assigning **appropriate individuals or teams with responsibilities and authorities** to carry out incident response activities and **ensuring that appropriate personnel are notified and available when needed**
- Defining **circumstances and mechanisms for reaching out to external personnel and experts**, as needed
- Establishing **notification thresholds and protocols** for informing regulators, customers, and law enforcement and communications strategies that define the "how, when, what, and who" of communicating to outside parties
- Assigning **appropriate authorities to personnel or teams to handle containment of the incident and restoration activities**
- Documenting and maintaining **incident evidence**, as well as the **decisions made and the actions taken** during the response
- Developing **required thresholds** for returning compromised services, equipment, and software to the network
- Defining circumstances for filing a **Suspicious Activity Report**[30]

The CSBS Ransomware Self-Assessment Tool (R-SAT) provides additional, more granular recommendations for specific incident response procedures, including:

- Monitoring **social media, hyper-local social media, and other news sources** for public awareness
- Implementing **out-of-band communications** to mitigate threat actor use of single sign-on (SSO) to access containment and remediation efforts
- Implementing **alternative strategies for connecting to critical third-party vendors** in the event of an incident
- Establishing **escalation procedures for enacting the business continuity/disaster recovery plans** in the event of significant or long-term impacts to operations

The FFIEC notes that, "Management should align incident response procedures with other related processes (e.g., cybersecurity, network operations, and physical security), outsourced services (e.g., contracted incident response obligations), and verify that the procedures are considered during planning and business continuity plan development."[31] Moreover, because of the wide variety of threats (ransomware, DDoS, business email compromise, etc.) potentially affecting the institution, the use of incident-specific response playbooks can more efficiently enable quicker response to the most likely or impactful types of attack and help to minimize disruption across the breadth of the institution.

The importance of testing and learning from real-world events

The incident response program and the incident response plan are not static by nature; they are living documents that require frequent updates. **Periodic testing of the incident response plan** is an essential exercise to ensure that the program and plan are accurate, up-to-date, and reliable when needed most. Testing also helps to ensure that individuals and teams charged with responsibilities in the IRP are familiar with their assignments. In the heat of an incident, well-trained personnel who are familiar with the IRP can reduce the likelihood that critical tasks are forgotten. IRP testing should address responses to a variety of incidents that the institution is most likely to experience and should involve all personnel with assigned responsibilities. In addition, testing events should ideally include senior management to ensure top-down awareness of response procedures, staff responsibilities, and general oversight needs in the event of an incident.

Experiences from real-world cyber events also provide the institution with perhaps the most beneficial opportunity to update the incident response program and incident response plan. Documentation of responses to an actual cyber incident (i.e., an after-action report) can cast a light on both strengths and weaknesses in the plan. Following an actual cyber incident, the institution should identify areas of the IRP that require adjustment (e.g., stale contact lists for vendors and response team members, duplication of duties and other response process issues, etc.).

Changes in vendors or staffing, the addition of new business units, or changes in the institution's technology environment are all events that necessitate a careful review of the incident response program. Cyber incidents can create near-instant chaos for the institution and discovering that the incident response program and plan are stale can mean the difference between an efficient, effective recovery and a disorganized response that can leave the institution floundering—especially when time is of the essence.

Any deficiencies identified from testing exercises, responses to real-world incidents, or changes in the institution's environment should be **tracked, prioritized and remediated appropriately**. Management should make any necessary changes to the incident response program and incident response plan with appropriate urgency to ensure that they are ready to deploy immediately in the event of an incident—even if these modifications are necessary between normal policy review and approval cycles.

Below are some questions you may ask management to ensure that the institution's incident response program is sufficient to allow the institution to satisfactorily respond to a cyberattack.

1 Does the institution's incident response plan identify an individual (internal or third-party) with the expertise to manage and coordinate all aspects of an incident?

WHY THIS IS IMPORTANT: Responding to a cyber incident can be chaotic, and time is often of the essence to ensure that the institution can successfully engage and work through its incident response plan. The incident response plan should identify an individual, either internally or through an engaged third party, who is well-versed and familiar with all aspects of the response process and can manage the complications that can arise from managing multiple teams of individuals performing different critical recovery duties. Although many individuals or teams will likely be carrying out separate duties during an incident, it is important that there is designated leadership for the entirety of the response process to ensure team coordination, inform management and the board, and address issues that arise in a timely manner.

2 Does the institution's written incident response plan address the following considerations:

a. **Defined circumstances when the plan is to be initiated**
b. **Assignment of roles and responsibilities for individuals and teams identified in the plan**
c. **Notification thresholds for informing regulators, customers, and law enforcement**
d. **Escalation procedures for enacting business continuity/disaster recovery plans in the event of significant or long-term impacts to operations**

WHY THIS IS IMPORTANT: The incident response plan itself can often be complex due to the many roles, responsibilities, and considerations it contains for management, operations, communications, and even technical response efforts. While a more comprehensive list of considerations is beyond the scope of this document (see the Incident Response Programs Fact Sheet), the considerations identified here define the circumstances for implementation of the plan when needed; who will be responsible for carrying out the plan when an incident occurs; when to notify regulators, customers, and law enforcement; and circumstances when enacting business continuity/disaster recovery plans becomes necessary to maintain continuity of operations during a significant incident.

3 Does management periodically test the incident response plan? Do tests involve individuals and teams with assigned responsibilities in the plan? Do testing efforts include senior management?

WHY THIS IS IMPORTANT: Periodic testing of the incident response plan is an absolutely essential exercise to ensure that the program and plan are accurate, up-to-date, and reliable when needed most. Testing also helps to ensure that individuals and teams charged with responsibilities in the plan are familiar with their assignments. In the heat of an incident, well-trained personnel who are intimately familiar with the plan can reduce the likelihood that critical tasks are duplicated or forgotten altogether. Plan testing should address responses to a variety of incidents that the institution is most likely to experience and should involve all personnel with assigned responsibilities. In addition, testing events should ideally include senior management to ensure top-down awareness of response procedures, staff responsibilities, and general oversight needs in the event of an incident.

4 Does management ensure that the incident response plan is reviewed and updated when changes in vendors or staffing, the addition of new business units, or changes the institution's technology environment occur? Is the plan also reviewed and updated, as needed, following testing exercises and after real-world implementation of the plan? Does management track and remediate deficiencies identified from testing exercises, responses to real-world incidents, and changes in the institution's environment?

WHY THIS IS IMPORTANT: Changes in vendors or staffing, the addition of new business units, or changes in the institution's technology environment are all events that necessitate a careful review of the incident response plan. **Experiences from real-world cyber events** also provide the institution with perhaps the most beneficial opportunity to update the incident response plan. Documentation of responses to an actual cyber incident (i.e., an after-action report) can cast a light on both strengths and weaknesses in the plan. Following an actual cyber incident, the institution should identify areas of the plan that require adjustment (e.g., stale contact lists for vendors and response team members, duplication of duties and other response process issues, etc.).

Any deficiencies identified from testing exercises, responses to real-world incidents, or changes in the institution's environment should be **tracked, prioritized and remediated appropriately**. Management should make any necessary changes to the incident response program and incident response plan with appropriate urgency to ensure that they are ready to deploy immediately in the event of an incident—even if these modifications are necessary between normal policy review and approval cycles.

IT ASSET MANAGEMENT (ITAM)

Why is IT asset management important?

Financial institutions are built around technology; therefore, it can be a real challenge to keep track of it all. As institutions continue to embrace technology for everyday operations, it becomes more and more critical to establish and maintain a firm handle on all assets in the institution's environment. An effective **IT asset management (ITAM) program** that manages all aspects of the asset life cycle is a cornerstone control that:

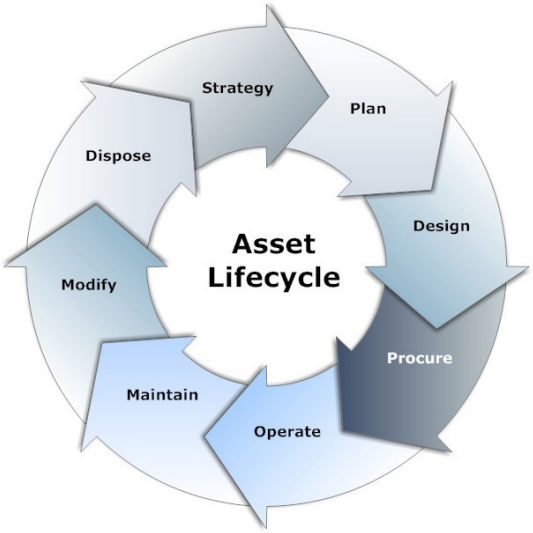
- Supports institutional risk management, including the development and maintenance of the information security program;
- Helps to enable the effective design, implementation, and troubleshooting of technology solutions and the mechanisms to secure them;
- Strengthens the effectiveness and comprehensiveness of patch management efforts; and
- Helps to ensure that end-of-life assets are properly identified and managed.

It is impossible for an institution to manage assets it does not know it has.

The IT asset life cycle

All IT assets—software, hardware, mobile devices, cloud assets, etc.—have a lifecycle. The following illustration from NIST provides a top-level overview of the lifecycle stages for IT assets.

The lifecycle begins with strategies and planning for acquiring or developing the asset and continues logically through the ongoing operation and maintenance of the asset, as well as any potential modifications that may be necessary over the course of its lifespan. The final stage of the lifecycle addresses the proper disposal of the asset at the end of its useful life.



Graphic Source: NIST

ITAM and risk management

Effective ITAM is a critical contributor to effective risk management practices throughout the institution. Robust technology asset inventories can assist in the **development of risk assessments** (e.g., information security, SOX, continuity and resilience, business unit, etc.) and can assist in compiling **audit risk assessments** and **building the audit universe and scope**.[32]

According to the FFIEC IT Handbook booklet: *Architecture, Infrastructure, and Operations,* "Management should have a comprehensive inventory of its electronic (or digital) and physical information assets to **adequately safeguard them against reasonably foreseeable threats**. An inventory will assist management as it develops and maintains the entity's **information security program** as described in the Information Security Standards."

ITAM helps to:

- Enable informed decision making required for **long-term planning**. When management is aware of its current inventory, they can better assess necessary design changes while ensuring that strategic goals align with the institution's distinct mission.
- Enable the **identification and acquisition of hardware and software that integrates best with the company's existing infrastructure**. This ensures both smooth scalability and avoids unnecessary business disruptions.[33]

Finally, effective ITAM processes and scanning tools can help to identify unauthorized IT devices, software, or other services, known as **"shadow IT,"** operating within the entity's environment or inside a third-party service provider's environment. According to the FFIEC, "Failure to address the risks of shadow IT may lead to an unknown attack vector due to management's lack of awareness of unapproved devices, software, or services." These risks may include, but are not limited to, security weaknesses, breaches, or loss of data from unapproved technology; an inability to accurately maintain and update shadow IT assets; and unintentionally backing up unmanaged devices, which may lead to the proliferation of malware throughout the network.[34]

ITAM is a foundation for vulnerability, patching, and end-of-life management programs

According to the FFIEC, "ITAM inventories help management know what systems need to be patched and the patch time frames, what hardware or software is nearing end-of-life, where the entity's vulnerability management focus should be, or when any additional security measures are necessary."[35]

Threat actors can quickly capitalize on even temporarily unpatched vulnerabilities in both software and hardware assets. Comprehensive, dynamically updated inventories of technology assets can help to make vulnerability identification and patching efforts more thorough, expedient, and effective. In fact, the success of the institution's patch management program is dependent, in part, on maintaining a dynamic, accurate inventory of assets that captures all new and existing technology assets making temporary or permanent connections to the network. Periodically reconciling detailed inventories of hardware and software assets is a form of version control that helps to ensure that patch management efforts are comprehensive and function properly.

ITAM processes can also ensure that any **end-of-life (EOL) assets** can be identified and managed appropriately within the institution. Because EOL assets are not supported by current security patches and updates from the vendor, they can introduce significant cyber risk. Moreover, EOL assets that are mission-critical systems require significant lead time to allow for the identification of acceptable mitigations and plans for replacement. An accurate inventory can, at a minimum, provide the institution with an accurate view of where these unsupported assets might be present and introducing unacceptable or unknown security risks.

ITAM considerations for hardware and software

A crucial component of asset inventory management is the **categorization of systems**. For hardware, it is important to differentiate between inventory owned and managed by third parties or owned and managed in house. Proper tracking of these assets includes assigning each one a unique identifier, such as serial numbers or asset tags. In addition, to classification of hardware, information about the entity's network and telecommunications equipment should be accounted for.[36]

Software inventory should also be kept accurate, providing detailed information about various applications and systems in use across the entity. This includes details such as, but not limited to, application criticality, version numbers, licensing details, patch level and patching date, and alignment of deployment status with licensing agreements.[37]

Depending on the size and complexity of the institution, **the methods and tools used to manage the hardware and software inventories will vary**. According to the FFIEC, "There are tools that may help management identify and manage hardware (including telecommunications) and software in the entity's IT environment. For example, automated asset management tools can scan an entity's IT environment for unauthorized hardware, software, and devices. Smaller or less complex entities may use manual asset inventory processes; these processes, however, should allow management to effectively document, track, and oversee the entity's technology assets."[38]

Below are some questions you may ask management to ensure that IT asset management (ITAM) practices are sufficient to support the institution's risk management, patch management, and end-of-life management programs.

1 Does the institution have an effective process to manage the full IT asset life cycle (from planning and procurement to disposal)?

WHY THIS IS IMPORTANT: All IT assets – software, hardware, mobile devices, cloud assets, etc.- have a life cycle, and management of each stage in the lifecycle is critical to maximize the value of the asset to the business and manage associated risk exposures for the life of the asset. The life cycle begins with strategies and planning for acquiring or developing the asset and continues logically through the ongoing operation and maintenance of the asset, as well as any potential modifications that may be necessary over the course of its lifespan. The final stage of the life cycle addresses the proper disposal of the asset at the end of its useful life.

2 Does the institution maintain an accurate, comprehensive, and dynamic inventory of all IT assets? Is it updated in real time and does it include hardware, software, cloud assets, and mobile devices?

WHY THIS IS IMPORTANT: Effective ITAM is a critical contributor to effective risk management practices throughout the institution. ITAM programs play a critical role in identifying **unauthorized IT devices, software, or other services** in the institution's environment and are instrumental to the comprehensiveness and success of **patch management** and **end-of-life management programs**.

3 How does ITAM align with the institution's overall business and IT strategy? Are asset decisions supporting digital transformation, sustainability, and cost optimization goals?

WHY THIS IS IMPORTANT: ITAM is a supporting mechanism for business strategies in that it helps to maximize the value of technology investments by ensuring that technology resources are aligned with the institution's organizational mission and goals, are efficiently used, and are properly governed. Strategically, ITAM gives the institution visibility into the entire asset management life cycle to better inform decisions about investment, cost optimization, and general risk management- both short-term and long-term. Effective ITAM also frees up resources to allow for growth and innovation within the institution.

4 What tools or products does the institution use to manage its IT asset inventory?

WHY THIS IS IMPORTANT: Depending on the size and complexity of the institution, the methods and tools used to manage the hardware and software inventories will vary. According to the FFIEC, "There are tools that may help management identify and manage hardware (including telecommunications) and software in the entity's IT environment. For example, automated asset management tools can scan an entity's IT environment for unauthorized hardware, software, and devices. Smaller or less complex entities may use manual asset inventory processes; these processes, however, should allow management to effectively document, track, and oversee the entity's technology assets." [39]

EVENT LOGGING & THREAT DETECTION

Why are proper logging practices important?

An institution's system event logging practices can provide increased visibility into system performance and compliance with established institutional security policies. In addition, strong logging practices often provide the first indicators of system incidents and compromise and can provide valuable support to incident response efforts. Visibility through logging should be considered immutable; without it, organizations cannot attribute or respond to cyber threats proactively, nor can they effectively investigate and reconstruct incidents after they occur. Ransomware and nation-state threat actors leverage **"living off the land"**, or **LOTL**, techniques to maintain hard-to-detect persistence in systems—sometimes for months at a time. The increased prevalence of malicious actors employing LOTL techniques further highlights the importance of implementing and maintaining an effective event logging solution.[40]

What are "living off the land" (LOTL) techniques?

In simple terms, "living off the land", or LOTL, techniques allow threat actors to leverage and abuse native tools and processes on systems, such as existing, legitimate binaries, that are already trusted in the institution's environment. Once a system or network has been compromised, these LOTL techniques allow the threat actor to conduct their operations discreetly by blending with typical system and network behavior, potentially eluding basic endpoint security capabilities. These techniques work very well for the threat actor because (a.) "many organizations lack effective security and network management practices (i.e., established baselines) that support detection of malicious LOTL activity; (b.) there is a general lack of conventional indicators of compromise (IOCs) associated with the activity, complicating network defenders' efforts to identify, track, and categorize malicious behavior; and (c.) it enables cyber threat actors to avoid investing in developing and deploying custom tools." Default logging configurations often do not comprehensively log indicators of LOTL techniques or provide sufficiently detailed information to differentiate malicious activity from normal, legitimate activity. In addition, system defenders may also find it difficult to identify a relatively small volume of malicious activity contained within vast amounts of log data.[41]

Countering LOTL techniques and improving logging and threat detection practices

There are four best practices identified to improve logging and threat detection practices and defend against the use of LOTL techniques associated with cloud services, enterprise networks, enterprise mobility, and operational technology (OT) networks: *Enterprise-approved event logging policy*, *centralized event log collection and correlation, secure storage and event log integrity,* and *detection strategy for relevant threats*.[42]

Enterprise-approved event logging policy

An enterprise-approved event logging policy increases consistency of logging practices throughout the organization and increases the chances of detecting malicious behaviors. This policy should consider any shared responsibilities between the institution and its service providers and should include "details of the events to be logged, event logging facilities to be used, how event logs will be monitored, event log retention durations, and when to reassess which logs are worthy of collection". The policy should focus on enabling the capture of "high quality cybersecurity events to aid network defenders in correctly identifying cybersecurity incidents". The policy should also address requirements that event logs be sufficiently detailed to enable forensic investigations and assist network defenders and incident responders. While developed as guidance for U.S. Federal Civilian Executive Branch agencies, the guidelines found in *US Office of Management and Budget's M-21-31 (OMB M-21-31)* document can provide useful guidance to financial institutions regarding specific data event logs should capture.[43] Logging practices should consider an appropriate degree of logging for OT devices and aim for consistency in content, format, and timestamping. Finally, log retention periods should ideally be driven by risk assessment of the subject system, and logs should be retained "long enough to support cybersecurity incident investigations". Effective logging solutions aim to reduce alert noise to increase savings on costs associated with storage and query time.[44] Prevailing guidelines for Federal agencies, as reflected in OMB M-21-31, require the retention of logs for 12 months (active storage) and 18 months (cold data storage).[45] Longer retention periods often equate to greater success in evaluating the scope of a cybersecurity incident.[46]

Centralized event log collection and correlation

The effectiveness of log monitoring can be enhanced through the centralization and correlation of event logs produced by various areas of the organization. *This enables prompt, efficient organization and identification of deviations from baselines, as well as cybersecurity events and incidents, through one continuous, centralized process.* Prioritization of logs from enterprise networks ideally focuses on logs from sources including, but not limited to, critical systems and data most likely to be targeted in an attack, internet-facing services, identity and domain servers, edge devices such as boundary routers and firewalls, admin workstations, and highly privileged systems and data repositories. In the OT environment (i.e., security systems, ATMs, point-of-sale systems, card personalization equipment, network-connected smart devices, etc.), areas for prioritization include those OT devices critical to safety and service delivery, internet-facing OT devices, and OT devices accessible via network boundaries. For mobile devices, logs from web proxies used by organizational users, organization operated DNS services, device security and behavior of organizationally managed devices, and user account behavior (e.g., sign-ins) should be prioritized in the organization's mobility solution. Finally, for cloud environments, organizations should adjust logging practices in line with the cloud service being administered (i.e., IaaS, SaaS, PaaS, etc.). Logs from critical systems and data most likely to be targeted; internet-facing services; tenant accounts that access and administer cloud services; logs for admin configuration changes; and logs for creating, modifying, and deleting security principles, including setting and changing permissions, should be prioritized.[47]

Secure storage and event log integrity

Cyber threat actors are known to target local system event logs for deletion or modification to "avoid detection and to delay or degrade the efficacy of cybersecurity incident response". Any log forwarding agents used by the institution should be properly secured and monitored. In addition, CISA recommends the use of cryptographic verification to ensure the integrity of event logs in-transit and at rest, prioritizing those records that have a justified requirement to record sensitive data. Access to delete, modify, or review audit logs should be limited to personnel with a justified requirement. Logs should ideally be stored in a separate or segmented network with additional security controls to help lessen the risk of tampering in the event of a network or system incident. Secure backup and data practices should also be implemented, and SIEMs should ideally be hardened and segmented from the general IT environment.[48]

...avoid detection and to delay or degrade the efficacy of cybersecurity incident response.

Detection strategy for relevant threats

CISA also recommends that organizations consider the implementation of user and entity behavioral analytics to better detect anomalous behavior on networks, devices, and accounts. A SIEM (security information and event management system) can detect unusual activity in the areas through the comparison of event logs to normal baseline business activity and traffic. The use of behavioral analytics can also be very helpful in detecting the use of LOTL techniques.[49]

Below are some questions you may ask management to ensure that event logging and threat detection processes are sufficient to address ongoing and emerging threats against the institution.

1 Does the institution have an enterprise-approved event logging policy?

WHY THIS IS IMPORTANT: According to CISA, an enterprise-approved event logging policy increases consistency of logging practices throughout the organization and increases the chances of detecting malicious behaviors. For financial institutions, this policy should:

- Consider any **shared responsibilities** between the institution and its service providers;
- Include **details** of the events to be logged, event logging facilities to be used, how event logs will be monitored, event log retention durations, and when to reassess which logs are worthy of collection;
- Focus on **capturing high quality cybersecurity events** to aid network defenders in correctly identifying cybersecurity incidents;
- Address requirements that event logs contain **sufficient detail to aid network defenders and incident responders**;
- Consider an appropriate degree of **logging for any network-connected operational technology (OT) devices** (i.e., security systems, ATMs, point-of-sale systems, card personalization equipment, network-connected smart devices, etc.) and aim for consistency in content, format, and timestamping; and
- Ideally be driven by **risk assessment of the subject system**.

Event logs should be detailed and retained long enough to support cybersecurity incident investigations and assist network defenders and incident responders. Longer retention periods often equate to greater success in evaluating the scope of a cybersecurity incident. The most effective logging solutions will aim to reduce alert noise to increase savings on costs associated with storage and query time.[50]

2 Does the institution have a process for the centralized collection and correlation of event logs produced from various areas of the institution (e.g., enterprise networks, operational technology (OT) networks, mobile devices, cloud environments)?

WHY THIS IS IMPORTANT: The effectiveness of log monitoring can be enhanced through the centralization and correlation of event logs produced by various areas of the organization. This enables prompt, efficient organization and identification of deviations from baselines, as well as cybersecurity events and incidents, through one continuous, centralized process. This centralization and correlation of log data considers inputs from areas such as enterprise networks, OT networks, mobile devices, and cloud environments. Moreover, within these areas, the institution should consider risk-based prioritization of inputs based on, but not limited to, logs for critical systems and data most likely to be attacked, areas considered critical to services and operations, internet-facing services, and logs for configuration changes and other administrative activity.[51]

3 Does the institution have a process to assure the security and integrity of local system event logs?

WHY THIS IS IMPORTANT: Cyber threat actors are known to target local system event logs for deletion or modification to elude detection and to delay or degrade the efficacy of the institution's incident response efforts.

- **Maintaining Data Integrity:** CISA recommends the use of cryptographic verification techniques to ensure the integrity of event logs in-transit and at rest, prioritizing those records that have a justified requirement to record sensitive data.
- **Access Control:** Access to delete, modify, or review audit logs should be limited to personnel with a justified requirement.
- **Log Storage:** Logs should ideally be stored in a separate or segmented network with additional security controls to help lessen the risk of tampering in the event of a network or system incident.
- **Log Backups and Security:** Secure backup and data practices should also be implemented, and security information and event management systems (SIEMs) should ideally be hardened and segmented from the general IT environment.[52]

4 Does the institution utilize user and entity behavioral analytics to detect anomalous behavior or activity on networks, devices, and accounts?

WHY THIS IS IMPORTANT: CISA recommends that organizations consider the implementation of user and entity behavioral analytics to better detect anomalous behavior on networks, devices, and accounts. A SIEM can detect unusual activity in the areas through the comparison of event logs to normal baseline business activity and traffic. The use of behavioral analytics can also be very helpful in detecting the use of *"living off the land",* or *"LOTL"* techniques, which are increasingly being used by both ransomware and nation-state threat actors to evade detection.

In simple terms, "living off the land", or LOTL, techniques allow threat actors to leverage and abuse native tools and processes on systems, such as existing, legitimate binaries, that are already trusted in the institution's environment. Once a system or network has been compromised, these LOTL techniques allow the threat actor to conduct their operations discreetly by blending with typical system and network behavior, potentially eluding basic endpoint security capabilities.[53]

MULTI-FACTOR AUTHENTICATION (MFA)

What is multi-factor authentication (MFA)?

A key security control that provides an enhanced means of verifying the identity of a user by requiring the user to provide two or more authentication factors (i.e., something you know, something you have, or something you are) at login.

Why is MFA important for your institution?

MFA increases the difficulty for threat actors to gain access to information systems via the use of compromised passwords or personal identification numbers (PINs). With MFA implemented, unauthorized users will be unable to access the account without providing a second verification factor. **This added layer of security is a crucial for stopping common malicious cyber activities (e.g., password spraying).**[54]

- A May 2023 Microsoft study revealed that the use of MFA "reduced the risk of compromise by 99.22% across the entire population and by 98.56% in the case of leaked credentials."[55]
- MFA is not a "magic bullet," nor a substitute for other security controls. However, recent FFIEC guidance on authentication states that, *"When a financial institution management's risk assessment indicates that single-factor authentication with layered security is inadequate, MFA or controls of equivalent strength as part of layered security can more effectively mitigate risks."*[56]

All MFA is NOT the same…

For MFA to be most effective, there are three primary considerations:

- ***The type of MFA to be used,***
- ***What assets MFA will be protecting within the organization, and***
- ***How MFA is configured.***

While the use of any form of MFA is preferable to using none, it is important to understand that there are multiple methods of implementing MFA, as well as variations in the degree of security provided by each MFA type.

- **SMS or Voice-Based Authentication**—*relies on codes sent to a user's phone or email*
  - According to CISA, this is the **weakest** form of authentication due to its susceptibility to phishing, exploitation of SS7 vulnerabilities, and SIM swapping. This form of authentication is generally viewed as a **last resort option and a temporary stopgap until stronger authentication methods can be implemented**.

- **Application-Based Authentication Without Number Matching**—*push prompts are received and accepted by a user to approve the request for access with no intermediate steps between the request and acceptance of approval*
  - This is a more secure method of MFA; however, this form of authentication is susceptible to push bombing attacks (flooding a user's device with access approval requests) and user error.

- **Application-Based Authentication Using One-Time Passwords (OTP), Mobile Push Notifications with Number Matching, or Token-Based OTP**—*requires an additional step(s) by the user (often the input of a one-time number).*
  - These methods provide an even higher degree of security for the authentication process and are **resistant** to push bombing attacks; however, these methods remain vulnerable to phishing attacks.

- **Phishing Resistant MFA**—includes FIDO or WebAuthn authentication and public key infrastructure (PKI) implementations
  - The "**gold standard**" for MFA. CISA urges system administrators and high-value targets to begin implementing or planning their migration to phishing resistant MFA.

WHERE you use MFA and HOW you configure it matters…

Like all other security controls, **where you use MFA and how it is configured** are important considerations. The implementation of MFA can be a complex process that requires careful planning and a phased approach.

> ***An asset with the weakest method of authentication becomes a potential path to bypass stronger authentication for a system that it is connected to.***
>
> - CISA

CISA recommends an organization-wide approach when implementing MFA as **it is more effective to implement MFA across all systems and applications instead of implementing redundant, isolated solutions for individual applications**. Further, it is important for management to identify systems in which MFA is not supported and develop plans for upgrading or migrating to systems that support MFA. The institution's risk assessment can help identify and prioritize areas where MFA application is needed. For organizations that elect to forego an organization-wide implementation of MFA, the primary areas of focus for implementation of MFA typically include, but are not limited to:

- Privileged access management (PAM) (domain administrative access, application administrative access, etc.)
- VPN/Remote Desktop (RDP) access into the network
- Vendor access into the network
- Access to any cloud-based service (email, mortgage origination, HR platforms, etc.)
- Access to external applications hosting nonpublic information (NPI)
- Situations where customers may be accessing NPI[57]

> ***To receive the full benefit of an MFA capability, organizations should be sure to implement it across all systems, applications, and resources.***
>
> - CISA

It is important that the chosen MFA technology is **configured properly, monitored, and supported by other security mechanisms** as part of layered security approach. Misconfigured or improperly managed MFA can provide a false sense of security and may create unintended weaknesses that may be easily exploited by cyber threat actors.

Below are some questions you may ask management to ensure MFA has been appropriately implemented to protect against cyber threats.

1 Has multi-factor authentication (MFA) been implemented in the institution? If so, does the institution rely on stronger application-based or phishing-resistant authentication methods (FIDO or public key infrastructure), as opposed to weaker SMS (text) or voice-based authentication?

WHY THIS IS IMPORTANT: MFA is a foundational security control that provides an enhanced means of verifying the identity of a system user by requiring the user to provide two or more authentication factors (i.e., something you know, something you have, or something you are) at login. While the use of any form of MFA is preferable to using none, it is important to understand that there are multiple methods of implementing MFA, as well as variations in the degree of security provided by each MFA type. In short, all MFA is not the same.

- SMS (text) and voice-based MFA methods are common but are the weakest form of authentication and, according to CISA, should ideally be used only as a temporary solution until stronger methods can be implemented in the institution.
- Stronger authentication methods include authentication via mobile push notification (with or without number matching); one-time passwords; and token-based one-time passwords.
- "Phishing-resistant" forms of MFA such as FIDO or WebAuthn authentication and public key infrastructure (PKI) authentication implementations are the gold standard for authentication and can generally offer superior protections against phishing, "push bombing", and other threats.

2 How has MFA been implemented?

- ☐ **For privileged access management (PAM) (domain administrative access, application administrative access, etc.)**
- ☐ **For all users that access any cloud-based service (mortgage origination, HR platforms, etc.)**
- ☐ **For cloud email services, such as Microsoft 365 and others**
- ☐ **For access to external applications hosting non-public information (NPI)**
- ☐ **For VPN/Remote Desktop (RDP) access into the network**
- ☐ **For vendor access into the network**
- ☐ **For internal service accounts**
- ☐ **For customers accessing NPI (e-Banking services, remote deposit capture, etc.)?**

WHY THIS IS IMPORTANT: MFA is implemented within an organization with a goal of strengthening authentication for critical systems and data, as well as protecting the institution against the use of stolen or "guessed" credentials. CISA recommends an organization-wide approach when implementing MFA as it is more effective to implement MFA across all systems and applications instead of implementing redundant, isolated solutions for individual applications. Further, it is important for management to identify systems in which MFA is not supported and develop plans for

upgrading these systems or migrating to new systems where MFA is supported. For organizations who elect to forego an immediate enterprise-wide implementation of MFA, the critical areas of focus for implementation of MFA typically include **privileged access management, email and other cloud-based services, applications that host nonpublic information, and remote access (including any vendor access) into the network, among others**.

3 Does the institution have a plan for future implementation of MFA to protect critical functions and data for areas where it is not currently implemented?

WHY THIS IS IMPORTANT: As previously mentioned, CISA recommends taking an organization-wide approach to the implementation of MFA. However, there are a number of factors, such as financial and operational concerns, that can limit an institution's ability to immediately implement an enterprise-wide solution. In these instances, an institution would be well served to carefully evaluate risk and prioritize areas, such as those mentioned above, where MFA implementation is warranted. Due to the potential financial and operational impacts of implementing an MFA solution, it is also advisable that the institution appropriately plan for implementation throughout critical areas via budgeting and strategic planning efforts.

4 Are MFA applications properly configured, monitored, and supported by other security mechanisms to afford expected protection?

WHY THIS IS IMPORTANT: MFA is not a "magic bullet", nor a substitute for other security controls when sensitive information is being protected. Recent FFIEC guidance on authentication states that, "When a financial institution management's risk assessment indicates that single-factor authentication with layered security is inadequate, MFA or controls of equivalent strength as part of **layered security** can more effectively mitigate risks." When MFA is implemented, it is important that the chosen technology is **configured properly, monitored, and supported by other necessary security mechanisms as part of a layered security approach**. Misconfigured or improperly managed MFA applications can provide a false sense of security to the institution and may create unintended weaknesses that may be easily exploited by cyber threat actors.

VULNERABILITY & PATCH MANAGEMENT

Why are vulnerability and patch management important?

Modern cyber criminals are opportunistic and extremely skilled at exploiting software and hardware vulnerabilities with lightning speed—sometimes before patches are even available. And the speed at which threat actors exploit these vulnerabilities will only continue to accelerate with the weaponization of artificial intelligence (AI) and other technologies. For context, approximately 28% of known exploitable vulnerabilities disclosed in 2024 were exploited within less than one day of their disclosure.[58] **Dynamic, comprehensive, and ongoing vulnerability and patch management programs** can help close the door to threat actor exploitation of software and hardware vulnerabilities across the organization.

For context, approximately 28% of known exploitable vulnerabilities disclosed in 2024 were exploited within less than one day of their disclosure.

What are the differences between vulnerability and patch management?

According to the FFIEC IT Handbook booklet: *Architecture, Infrastructure, and Operations*, vulnerability management is "a process to continuously acquire, assess, and take action on new information to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers. **Part of vulnerability management is patch management.** Patch management is the systematic notification, identification, deployment, installation, and verification of OS and application software code revisions."[59]

Part of vulnerability management is patch management.

Vulnerability management basics

At its core, vulnerability management addresses the identification and remediation of risks specific to your institution. The FFIEC notes that, "To have systems that are operationally functional and secure and perform as intended, management should implement a vulnerability management program that identifies systems and software vulnerabilities, prioritizes the vulnerabilities and the affected systems in order of risk, and performs timely remediation, according to the risk associated with the system. The program should include an entity's systems and software operating in the cloud for which the entity is responsible and those managed by the entity on its premises."[60]

Third-party information sources and scanning tools

To help the institution better understand the nature of threats, it is important to integrate relevant threat information into the vulnerability management program. This can be accomplished through the **monitoring of third-party information sources**, such as FS-ISAC, NIST, regulatory and law enforcement alerts, and trusted vendor partners. The FFIEC also states that, "Management should implement a process to periodically assess systems and software for vulnerabilities using scanners that are updated with a current vulnerability list."[61] The effectiveness of scanning efforts is dependent on the existence of a comprehensive inventory of approved systems, software, and devices. Scans should "include all systems and software in the entity's hardware, software, and telecommunications inventories." Proper controls should be in place to protect these scanning tools "against unauthorized use or access to sensitive information", including "separation of duties, logical security, configuration management, and log review."[62] Further, scans should ideally be agent-based or authenticated for higher-confidence results.

Vulnerability management goes beyond systems and software assets

When thinking of vulnerability management, it is important to recognize that **vulnerabilities are not limited to systems or software assets**. Vulnerability management also encompasses weaknesses in "security procedures, physical layout, or internal controls that malicious users could exploit to gain unauthorized access to systems or information or to disrupt critical services."[63]

Patch management basics

The FFIEC IT Handbook booklet, *Information Security,* provides a number of processes and controls to address patch management in the institution. Considerations include the following:

- **A monitoring process that identifies the availability of software (and hardware) patches.** This process should be timely and present a comprehensive view of available patches that refreshes frequently as new patches are introduced. The patching process should be built upon a comprehensive inventory of hardware and software assets to ensure thoroughness in the patching process. Patching programs should cover the entire security stack, including hardware, software, cloud-based assets, and containers.

- **A process to evaluate the patches against the threat and network environment.** This process will allow the institution to tailor the application of patches to its own unique environment and will assist in the prioritization of patches by severity and potential impact to the institution.
- **A prioritization process to determine which patches to apply across classes of computers and applications.** Patches should ideally be prioritized based upon severity, with Known Exploited Vulnerabilities (KEVs), critical, and high-severity vulnerabilities receiving the most urgent priority in the institution's patching regimen. Ideally, "critical" vulnerabilities should be remediated within 15 calendar days of initial detection; "high" severity vulnerabilities should be remediated within 30 calendar days.[64] Institutions should also be aware of smaller remediation windows that may be recommended by vendors to remediate more urgent vulnerabilities. In the event a vendor fails to assign a rating to a specific vulnerability, the institution should perform internal threat modeling or consult external sources, such as FS-ISAC, to determine prioritization for remediating the vulnerability.
- **A process for obtaining, testing, and securely installing patches, including in the institution's virtual environments.** Once the institution has identified and prioritized necessary patches, it is necessary to retrieve patches from the vendor. Testing patched applications in a controlled, non-production environment can more safely reveal how changes to a patched asset might interact with or create conflicts in the operating environment prior to enterprise-wide deployment.
- **An exception process, with appropriate documentation, for patches that management decides to delay or not apply.** There are occasionally circumstances where patches may not be readily applicable within the institution's environment (e.g., when unacceptable interoperability conflicts occur, etc.). Documenting and tracking unapplied patches can help management understand the nature of any issues noted, as well as any necessary plans for remediation, including the application of compensating controls, until issues can be resolved.
- **A process to ensure that all patches installed in the production environment are also installed in the disaster recovery environment in a timely manner.** The institution should ensure that all patches installed in the production environment are mirrored in the disaster recovery environment to ensure security and consistency should a failover become necessary.
- **A documentation process to ensure the institution's information assets and technology inventory and disaster recovery plans are updated as appropriate when patches are applied.** Patching can introduce new features, updated version numbers, changes to dependencies, or even compatibility issues within the institution's environment. Documentation of patch changes can help to ensure that the institution is fully aware of the current state of its inventory and that its disaster recovery plans are reflective of the current state of assets in the environment.[65]

Below are some questions you may ask management to ensure appropriate, comprehensive vulnerability and patch management practices have been implemented to protect against cyber threats.

1 What resources are leveraged to understand the nature of threats to the institution? Does the institution receive ongoing threat information from reliable sources, such as FS-ISAC, NIST, regulatory and law enforcement alerts, and trusted vendor partners? Does the institution maintain an ongoing process to periodically scan systems and software for vulnerabilities?

WHY THIS IS IMPORTANT: To help the institution better understand the nature of threats, it is important to integrate relevant threat information into the vulnerability management program. This can be accomplished through the **monitoring of third-party information sources**, such as FS-ISAC, NIST, and regulatory and law enforcement alerts. Threat information from these third-party sources should ideally be integrated into the institution's asset scanning programs. The FFIEC's Information Technology Handbook booklet, Architecture, Infrastructure, and Operations, states that "**management should implement a process to periodically assess systems and software for vulnerabilities using scanners that are updated with a current vulnerability list".** The effectiveness of scanning efforts is dependent on the existence of a comprehensive asset inventory of approved systems, software, and devices, and *scans should include all systems and software in the institution's hardware, software, and telecommunications inventories. Proper controls, including separation of duties, logical security, configuration management, and log review should be in place to protect these scanning tools against unauthorized use or access to sensitive information.*[66] Scans should ideally be agent-based or authenticated for higher-confidence results.

2 Does the institution have an established process for identifying available software and hardware patches, and does the institution actively evaluate those patches against the threat and network environment?

WHY THIS IS IMPORTANT: Patches for software and hardware assets, including patches to address critical security vulnerabilities, are released frequently. This process should be timely and present a comprehensive view of available patches that refreshes frequently as new patches are introduced. In addition, available patches should be evaluated against the institution's threat and network environment. This process will allow the institution to tailor the application of patches to its own unique environment and will assist in the prioritization of patches by severity and potential impact to the institution.[67]

3 Does the institution have a process to address the prioritization of patches that identifies which patches to apply across classes of computers and applications? Is there a process for obtaining, testing, and securely installing patches, including those applicable to the institution's virtual environment?

WHY THIS IS IMPORTANT: Patches should ideally be prioritized based upon severity, with Known Exploited Vulnerabilities (KEVs), critical, and high-severity patches receiving the most urgent priority in the institution's patching regimen. **CISA notes that "critical" vulnerabilities should be remediated within 15 calendar days of initial detection; "high" severity vulnerabilities should be remediated within 30 calendar days.**[68] Institutions should also be aware of smaller remediation windows that may be recommended by vendors to remediate more urgent vulnerabilities. In the event a vendor fails to assign a rating to a specific vulnerability, the institution should perform internal threat modeling or consult external sources, such as FS-ISAC, to determine prioritization for remediating the vulnerability.

Once the institution has identified and prioritized necessary patches, it is necessary to retrieve patches from the vendor. Testing patches in a controlled, non-production environment can more safely reveal how changes to a patched asset might interact with or create conflicts in the operating environment prior to enterprise-wide deployment.[69]

4 Does the institution actively track any patches or security updates that management chooses to delay or not apply? Is there a process to document and track these exceptions? Have sufficient compensating controls been applied to any unpatched assets that exist within the institution?

WHY THIS IS IMPORTANT: There are occasionally circumstances where patches may not be readily applicable within the institution's environment (e.g., when unacceptable interoperability conflicts occur, etc.). Documenting and tracking unapplied patches can help management understand the nature of any issues noted, as well as any necessary plans for remediation, including the application of compensating controls, until issues can be resolved.[70]

5 Does the institution ensure that any patches applied in the production environment are also applied in the disaster recovery environment in a timely manner? Is there a documentation process to ensure the institution's information assets and technology inventory and disaster recovery plans are updated as appropriate when patches are applied?

WHY THIS IS IMPORTANT: The institution should ensure that all patches installed in the production environment are mirrored in the disaster recovery environment to ensure security and consistency should a failover become necessary. In addition, patching can introduce new features, updated version numbers, changes to dependencies, or even compatibility issues within the institution's environment. Documentation of patch changes can help to ensure that the institution is fully aware of the current state of its inventory and that its disaster recovery plans are reflective of the current state of assets in the environment.[71]

THREAT INTELLIGENCE PROGRAMS

Why are threat intelligence programs important?

Individual threat actors and organized threat groups continue to attack financial institutions with increasingly sophisticated tools, sometimes backed by organized crime or even nation-state support. According to NIST, "Threat actors can be persistent, motivated, and agile, and they use a variety of tactics, techniques, and procedures (TTPs) to compromise systems, disrupt services, commit financial fraud, and expose or steal intellectual property and other sensitive information. Given the risks that these threats present, it is increasingly important that organizations share cyber-threat information and use the community's experience to improve their security posture." Properly developed and implemented **threat intelligence programs** help financial institutions gather, analyze, and act upon threat information before negative impacts occur. **Intelligence gathering and sharing** is a proactive process to stay ahead of attacks, whether it's a phishing campaign targeting employees, a ransomware event, or a nation-state threat actor probing the institution's network and systems. Without threat intelligence, institutions are effectively "flying blind" to a host of ever-changing and potentially devastating cyber threats.

Without threat intelligence, institutions are effectively "flying blind" to a host of ever-changing and potentially devastating cyber threats.

Threat intelligence program basics

Good threat intelligence programs contain four basic elements:

- **Information obtained from a trusted source,**
- **Channels to distribute information to the appropriate IT security personnel,**
- **Program to analyze and prioritize information based on the institution's own unique needs, and**
- **Acting upon applicable information in a timely manner.**

Types of threat information

NIST defines **"cyber-threat information"** as "any information that can help an organization to identify, assess, monitor, and respond to cyber-threats. These include:

- ***Indicators***, which are the system artifacts or observables that may suggest an attack is imminent, underway, or has already occurred;
- ***Tactics, techniques, and procedures (TTPs)***, which describe threat actor behavior;
- ***Security alerts, advisories, or bulletins***, which provide notification of vulnerabilities, exploits, and other security issues;
- ***Threat intelligence reports***, which are "prose documents" that describe TTPs, actors, targets, and other threat information; and
- ***Tool configurations***, which give recommendations for setting up and using automated collection, exchange, processing, analysis, and use of threat information.[72]

Threat intelligence resources

There are a variety of free and paid threat intelligence resources that financial institutions can leverage to gather this information. The most common sources include, but are not limited to:

- FS-ISAC and MS-ISAC: Information-sharing communities that deliver real-time alerts and sector-specific intelligence. U.S. institutions with less than $1B in assets can maintain a cost-free membership with FS-ISAC's Critical Notification Only Participant (CNOP) program.
- FBI InfraGard: Connects financial institutions with law enforcement for information sharing and early warnings
- CISA Programs and Alerts: Offers updates on vulnerabilities, malware campaigns, and best practices from the U.S. government
- Open Threat Exchange (OTX) and other community-driven threat exchange platforms
- Subscriptions to newsfeeds from industry cybersecurity websites
- Communications and alerts sent directly from applicable hardware and software vendors
- Vendor-sponsored CISO user groups

Understanding the institution's technology environment

Having a **mechanism to manage the myriad available threat information** is essential to navigate through the noise of irrelevant or untimely information. To make the most sense of threats that might impact the institution, it is important to remember a couple of key requirements. First, it is extremely beneficial to understand the institution's own operating environment. **Not all threats and vulnerabilities are applicable to every institution**, and the best way to sift through the noise that can accompany threat intelligence gathering is to understand the threats that are most relevant to your institution.

Second, when we think of potential impacts of threats, it is helpful to also understand the **interactions that assets have with one another within the institution's operating environment**. Is there an understanding of interdependencies between assets across different areas of the institution? Are there multiple areas within the institution that rely on a single application or piece of hardware (single point of failure)? Understanding not only the threats that exist, but also how these threats, if materialized, might impact overall operations is a good means of **triaging threat information and prioritizing responses and preparing recovery strategies for mission critical processes** within the institution. Because threats often require swift actions, it is important that IT security teams are well-equipped to **act upon threat intelligence information** once it's received, analyzed, and prioritized. Threat intelligence can provide timely data to enhance threat modeling activities for critical assets and can be a valuable input for incident and recovery scenario planning.

Information sharing

According to NIST, "Most organizations already produce multiple types of cyber-threat information that are available to share internally as part of their IT and security operations efforts." **When a financial institution participates in an information sharing mechanism, others benefit from "the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats the organization may face.** Using this knowledge, an organization can make threat-informed decisions regarding defensive capabilities, threat detection techniques, and mitigation strategies." Moreover, "By correlating and analyzing cyber-threat information from multiple sources, an organization can also enrich existing information and make it more actionable. Organizations that receive threat information and subsequently use this information to remediate a threat confer a degree of protection to other organizations by impeding the threat's ability to spread." Resources such as NIST Special Publication (SP) 800-150, Guide to Cyber-Threat Information Sharing, can assist institutions in forming and participating in cyber-threat information sharing activities.

Below are some questions you may ask management to ensure that the institution has a threat intelligence program that allows the institution to gather, analyze, and act upon threat information before negative impacts occur.

1 How does the institution gather, analyze, and act on threat intelligence?

WHY THIS IS IMPORTANT: There are a variety of threat intelligence resources that financial institutions can leverage to gather this information. The most common sources include, but are not limited to:

- FS-ISAC and MS-ISAC: Information-sharing communities that deliver real-time alerts and sector-specific intelligence. U.S. institutions with less than $1B in assets can maintain a cost-free membership with FS-ISAC's Critical Notification Only Participant (CNOP) program.
- FBI InfraGard: Connects financial institutions with law enforcement for information sharing and early warnings
- CISA Programs and Alerts: Offers updates on vulnerabilities, malware campaigns, and best practices from the U.S. government
- Open Threat Exchange (OTX) and other community-driven threat exchange platforms
- Subscriptions to newsfeeds from industry cybersecurity websites
- Communications and alerts sent directly from applicable hardware and software vendors
- Vendor-sponsored CISO user groups

It is important to have a process to disseminate threat information to appropriate IT/Security personnel in a timely manner.

2 Does the institution's threat intelligence program incorporate a process for managing and acting upon threat information?

WHY THIS IS IMPORTANT: Having a **mechanism to manage the myriad available threat information** is essential to navigate through the noise of irrelevant or untimely information. To really make the most sense of threats that might impact the institution, it is important to remember a couple of key requirements. First, it is extremely beneficial to **understand the institution's own operating environment,** as well as **interactions that assets have with one another within the institution's operating environment.** The point is that there is not always a singular effect on a specific asset when threats materialize. Understanding not only the threats that exist, but also how these threats, if materialized, might impact overall operations is a good means of **triaging threat information and prioritizing responses and preparing recovery strategies for mission critical processes** within the institution. And because threats often require swift actions to address, it is important that IT security teams are well-equipped to **act upon threat intelligence information** once it's received, analyzed, and prioritized.

3 Does the institution participate in an information-sharing organization to receive and share threat information?

WHY THIS IS IMPORTANT: According to NIST, "Most organizations already produce multiple types of cyber-threat information that are available to share internally as part of their IT and security operations efforts." **When a financial institution participates in an information sharing mechanism, others benefit from "the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats the organization may face.** Using this knowledge, an organization can make threat-informed decisions regarding defensive capabilities, threat detection techniques, and mitigation strategies. By correlating and analyzing cyber-threat information from multiple sources, an organization can also enrich existing information and make it more actionable. Organizations that receive threat information and subsequently use this information to remediate a threat confer a degree of protection to other organizations by impeding the threat's ability to spread."[73]

4 Are we conducting regular threat scenario planning based on the top threats to our institution?

WHY THIS IS IMPORTANT: The vast majority of IT assets used in financial institutions today are exposed to a constantly changing and perpetually dangerous threat environment. Threat modeling allows the institution to leverage intelligence to **help identify specific threats to critical assets or processes and design and test specific countermeasures to lessen the risk from these threats.** In addition, this same threat intelligence can also help **to inform the institution's incident and recovery scenario planning processes.** The goal is to recognize cyber threat-borne risks before they materialize, and robust, dynamic threat intelligence programs can be a principal driver in the success of these efforts across the entirety of the organization.

> ***Most organizations already produce multiple types of cyber-threat information that are available to share internally as part of their IT and security operations efforts.***

THIRD-PARTY RISK MANAGEMENT (TPRM)

Why is third-party risk management important?

Financial institutions do not operate in a vacuum. Institutions rely on service providers and other third-party vendors to help with everything from the most mundane administrative tasks to the most mission-critical activities. And it's this reliance that makes managing these relationships so critically important. Furthermore, as third-party artificial intelligence (AI) solutions continue to emerge and find their way into financial institutions, the need for diligent vendor risk management practices will only continue to increase. A sound **third-party risk management (TPRM) program** that actively addresses all stages of the third-party relationship life cycle is the foundation for identifying, managing, and mitigating these existing and emerging risks.

Interagency Guidance on Third-Party Relationships: Risk Management

In June 2023, the federal banking agencies released *Interagency Guidance on Third-Party Relationships: Risk Management*, which "offers the agencies' views on sound risk management principles for banking organizations when developing and implementing risk management practices for all stages in the life cycle of third-party relationships. The final guidance also provides some foundational considerations for third-party relationship management, including the following:

- **Sound third-party risk management takes into account the level of risk, complexity, and the size of the banking organization and the nature of the third-party relationship.**
- **A banking organization's use of third parties does not diminish its responsibility to meet these requirements to the same extent as if its activities were performed by the banking organization in-house.**
- **Sound risk management includes an analysis of risk with each relationship and tailored risk management practices commensurate with the banking organization's size, complexity, and risk profile and with the nature of the third-party relationship.**

While the aforementioned regulatory guidance applies to banking institutions, the principles outlined here are **equally important for nonbank financial institutions** as well—particularly in view of service provider oversight requirements contained in the Federal Trade Commision's Safeguards Rule.

Third-party risk management governance

Management of third-party relationships can be complex, depending on the volume, complexity, and risk associated with the institution's portfolio of relationships. **Oversight and accountability for the TPRM process ultimately lies with the institution's board of directors**, which provides "clear guidance regarding acceptable risk appetite, approves appropriate polices, and ensures that appropriate procedures and practices have been established." Similarly, management is responsible for "developing and implementing third-party risk management policies, procedures, and practices, commensurate with the banking organization's risk appetite and the level of risk and complexity of its

third-party relationships." The interagency guidance notes that, "It is important for a banking organization to conduct **periodic independent reviews to assess the adequacy of its third-party risk management processes**." Finally, **thorough documentation and reporting of third-party risk management processes** is also important to "assist those within or outside of the banking organization who conduct control activities."

The third-party risk management life cycle

Generally, third-party relationships follow a logical life cycle:

- Planning
- Due diligence and third-party selection
- Contract negotiation
- Ongoing monitoring
- Termination[74]

Graphic Source: Board, FDIC, and OCC

Planning

At its core, the **planning stage** "allows a banking organization to evaluate and consider how to manage risks before entering into a third-party relationship." Considerations in the planning stage include:

- Evaluation of the strategic purpose of the relationship and its alignment with, among other things, the institution's overall goals, risk appetite, and corporate policies
- Benefits and risks of the relationship
- Nature of the relationship (activity volume, technology needed, etc.)
- Relationship costs
- Impact on employees
- Potential physical and information security implications
- How the institution will select, assess, and oversee the third party
- Ability to provide adequate oversight
- Contingency plans for exiting the relationship[75]

Due diligence and third-party selection

Pre-selection due diligence allows the institution to "determine if a relationship would help achieve a banking organization's strategic and financial goals", and "provides the banking organization with the information needed to evaluate whether it can appropriately identify, monitor, and control risks associated with the particular third-party relationship. Relying solely on experience with or prior knowledge of a third party is not an adequate proxy for performing appropriate due diligence, as due diligence should be tailored to the specific activity to be performed by the third party." Due diligence considerations for prospective relationships include:

- Strategies and goals of the third party
- Legal and regulatory compliance
- Financial condition
- Business experience
- Qualifications and background of key personnel
- Risk management effectiveness
- Information security implications
- Business processes and management information systems
- Operational resilience
- Incident reporting and management processes
- Physical security
- Reliance on subcontractors
- Insurance coverage
- Contractual arrangements with other parties[76]

Contract negotiation

Once the institution performs its initial due diligence and chooses to enter into a relationship with a third party, the institution (in conjunction with legal counsel, if warranted) will determine whether the relationship warrants a formal contract and, if so, **negotiates contract terms** that "will facilitate effective risk management and oversight and that specify the expectations and obligations" of both parties. Considerations for negotiating an appropriate contract include:

- Nature and scope of the arrangement
- Well-defined performance measures or benchmarks
- Responsibilities for providing, receiving, and retaining information
- Right to audit and require remediation
- Responsibility for compliance with applicable laws and regulations
- Costs and compensation
- Ownership and license

- Confidentiality and integrity
- Operational resilience and business continuity
- Indemnification and limits on liability
- Insurance
- Dispute resolution and customer complaints
- Use of subcontractors
- Provisions for foreign-based third parties (where applicable)
- Default and termination terms
- Considerations for regulatory supervision[77]

Ongoing monitoring

A critical step in the TPRM life cycle model is the **ongoing monitoring of third-party relationships**. Once the institution has entered into the relationship, ongoing monitoring of the relationship "enables a banking organization to: (1) confirm the quality and sustainability of a third party's controls and ability to meet contractual obligations; (2) escalate significant issues or concerns, such as material or repeat audit findings, deterioration in financial condition, security breaches, data loss, service interruptions, compliance lapses, or other indicators of increased risk; and (3) respond to such significant issues or concerns when identified." This monitoring, as with other aspects of the TPRM life cycle, should be "commensurate with the level of risk and the complexity of the relationship and the activity performed by the third party. Ongoing monitoring may be conducted on a periodic or continuous basis, and more comprehensive or frequent monitoring is appropriate when a third-party relationship supports higher-risk activities, including critical activities." Considerations for the ongoing monitoring of relationships include:

- Effectiveness of the relationship
- Changes to the third party's business strategies and agreements with other entities
- Changes in financial condition
- Changes to or lapses in insurance coverage
- Audits, testing results, and other reports
- Ongoing compliance with laws and regulations
- Changes in key personnel
- Reliance on subcontractors
- Training; responses to new threats, vulnerabilities, and incidents
- Ability to maintain confidentiality, integrity, and availability of systems and data
- Business resiliency capabilities
- External factors that might impact the third party
- Volume and nature of complaints against the third party.[78]

Termination

There are instances where an institution may elect to **sever a relationship** with a third party. This might be due to a breach of contract, a failure of the third party to comply with laws or regulation, or simply because the institution wants to move in a different direction. However, simply severing a relationship with a third party isn't always easy. Depending on the nature and complexity of the relationship, there are a number of factors to consider, including:

- Options to facilitate the transition of services
- Capabilities, resources, and timeframes for transitioning
- Costs and fees associated with the termination
- Management of risks associated with data retention and destruction, access control, and connections with systems
- Joint intellectual property issues
- Management of risks to the institution and its customers if termination occurs due to the third party's inability to meet institutional expectations.[79]

Third-party risk management and emerging technologies

The continued emergence of AI and other technologies has provided institutions with a glimpse into new efficiencies, cost savings, and even improvements to the customer experience. However, as with the integration of any technology into the institution's environment, appropriate product and vendor due diligence is necessary to ensure that the technology **meets the institution's strategic and operational needs** and **does not introduce unacceptable risks to the institution**. In the early stages of the new technology life cycle, new products- as well as their vendors- may be numerous but may also lack the maturity and experience associated with long-standing technologies and providers. For these reasons, the utilization of strong third-party risk management practices is essential to ensure that new relationships with emerging technology providers and their products are beneficial, well-understood, and secure for the organization and its customers.

Below are some questions to ask management to ensure that the institution's third-party risk management program addresses all stages of the third-party relationship life cycle for its vendors and service providers.

1 Does the institution's TPRM program and policy address the planning stage of the TPRM life cycle?

WHY THIS IS IMPORTANT: At its core, the **planning stage** of the TPRM life cycle "allows a banking organization to evaluate and consider how to manage risks before entering into a third-party relationship." Considerations in the planning stage include, among other things, whether the proposed relationship strategically aligns with the institution's goals, risk appetite, and policies; benefits and risks of the relationship; the nature of the relationship; costs and potential impact to employees; and the ability to provide adequate oversight of the relationship.[80]

2 Does the TPRM program and policy address due diligence and selection requirements for prospective third-party relationships?

WHY THIS IS IMPORTANT: Pre-selection due diligence allows the institution to "determine if a relationship would help achieve a banking organization's strategic and financial goals", and "provides the banking organization with the information needed to evaluate whether it can appropriately identify, monitor, and control risks associated with the particular third-party relationship. Relying solely on experience with or prior knowledge of a third party is not an adequate proxy for performing appropriate due diligence, as due diligence should be tailored to the specific activity to be performed by the third party." Important due diligence considerations include, among other things, the financial condition and business experience of the vendor or service provider, information security implications, vendor resilience, and reliance on subcontractors.[81]

3 Does the TPRM program and policy address the negotiation of contracts?

WHY THIS IS IMPORTANT: Once the institution performs its initial due diligence and chooses to enter into a relationship with a third party, the institution (in conjunction with legal counsel, if warranted) will determine whether the relationship warrants a formal contract and, if so, **negotiates contract terms** that "will facilitate effective risk management and oversight and that specify the expectations and obligations" of both parties. Typical considerations for negotiation include the nature and scope of the agreement; well-defined performance measures or benchmarks; responsibilities for providing, receiving, and retaining information; costs and compensation; data confidentiality and integrity; use of subcontractors; dispute resolution; and default and termination terms.[82]

4 Does the TPRM program and policy address the ongoing monitoring of third-party relationships?

WHY THIS IS IMPORTANT: Ongoing monitoring of the relationship "enables a banking organization to:

a. Confirm the quality and sustainability of a third party's controls and ability to meet contractual obligations;

b. Eescalate significant issues or concerns, such as material or repeat audit findings, deterioration in financial condition, security breaches, data loss, service interruptions, compliance lapses, or other indicators of increased risk; and

c. Respond to such significant issues or concerns when identified." This monitoring, as with other aspects of the TPRM life cycle, should be commensurate with the level of risk and the complexity of the relationship and the activity performed by the third party.

Further, "Ongoing monitoring may be conducted on a periodic or continuous basis, and more comprehensive or frequent monitoring is appropriate when a third-party relationship supports higher-risk activities, including critical activities." Considerations for the ongoing monitoring of relationships include, among other things, an evaluation of the effectiveness of the relationship; changes in financial condition; ongoing compliance with laws and regulations; changes in key personnel; reliance on subcontractors; and the ability to maintain the confidentiality, integrity, and availability of systems and data.[83]

5 Does the TPRM program and policy address the termination of third-party relationships?

WHY THIS IS IMPORTANT: There are instances where an institution, for a variety of reasons, may elect to **terminate a relationship** with a third party. Simply severing a relationship with a third party isn't always easy. Depending on the nature and complexity of the relationship, there are a number of factors to consider including, but not limited to, options to facilitate the transition of services; capabilities, resources, and timeframes for transitioning; costs and fees associated with the termination of services; management of risks associated with data retention, access control and system connections; and impacts to the institution and its customers if termination occurs due to the third party's inability to meet institutional expectations.[84]

WORKS CITED

1 CISA. Press Release: CISA Unveils New Public Service Announcement—We Can Secure Our World. May 2024.

2 Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency. Interagency Guidance on Third-Party Relationships: Risk Management. June 2023.

3 Mimecast. *The State of Human Risk 2025*, p.5.

4 Chew, Tan Soon (ISACA). "Considerations for Developing Cybersecurity Awareness Training", March 1, 2023.

5 Lewis, Jon (Cira). "How to Measure a Phishing Test Program", January 6, 2024.

6 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Information Security—II.C.7.(e)—Training. September 2016.

7 CSBS. *CSBS Ransomware Self-Assessment Tool for Banks, Version 2.0.* October 24, 2023.

8 Ibid.

9 Chew, Tan Soon (ISACA). "Considerations for Developing Cybersecurity Awareness Training", March 1, 2023.

10 Lewis, Jon (Cira). "How to Measure a Phishing Test Program", January 6, 2024.

11 CSBS. CSBS Ransomware Self-Assessment Tool for Banks, Version 2.0. October 24, 2023.

12 Ibid.

13 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - VI.B.4- Backup and Replication Processes. June 2021.

14 IBM (Flinders, Mesh and Smalley, Ian). *"What is an air gap?"*. October 14, 2024.

15 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Business Continuity Management Booklet—IV.A.3—Data Backup and Replication. November 2019.

16 Ibid.

17 Ibid.

18 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - VI.B.4- Backup and Replication Processes. June 2021.

19 IBM (Flinders, Mesh and Smalley, Ian). "What is an air gap?". October 14, 2024.

20 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Business Continuity Management Booklet – IV.A.3 – Data Backup and Replication. November 2019.

21 Ibid.

22 Ibid.

23 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - VI.B.4- Backup and Replication Processes. June 2021.

24 Todd, H. (Yorb). *The Consequences of Ignoring End-of-Life Systems and Hardware,* July 31, 2023.

25 FFIEC. *FFIEC Information Technology Examination Handbook: Information Security - II.C.11 End-of-Life Management,* September 2016.

26 Ibid.

27 Ibid.

28 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Information Security - III.D - Incident Response. September 2016.

29 National Institute of Standards and Technology. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. April 2025.

30 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Information Security - III.D - Incident Response. September 2016.

31 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Business Continuity Management - V.F.1 - Incident Response. November 2019.

32 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - III.B.1 - Technology Asset Inventory. June 2021.

33 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - III.B - IT Asset Management. June 2021.

34 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - III.B.3 - Shadow IT. June 2021.

35 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - III.B - IT Asset Management. June 2021.

36 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - III.B.1(a) - Hardware Inventory. June 2021.

37 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - III.B.1(b) - Software Inventory. June 2021.

38 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - III.B.1 - Technology Asset Inventory. June 2021.

39 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - III.B.1 - Technology Asset Inventory. June 2021.

40 CISA (Jointly with NSA, FBI, and others). *Best Practices for Event Logging and Threat Detection*. August 22, 2024.

41 CISA (Jointly with NSA, FBI, and others). *Joint Guidance: Identifying and Mitigating Living off The Land Techniques.* February 7, 2024.

42 CISA, August 22, 2024.

43 US Office of Management and Budget. *Memo M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*. August 27, 2021.

44 CISA. August 22, 2024.

45 US Office of Management and Budget. August 27, 2021.

46 CISA. August 22, 2024.

47 Ibid.

48 Ibid.

49 Ibid.

50 CISA (Jointly with NSA, FBI, and others). Best Practices for Event Logging and Threat Detection. August 22, 2024.

51 Ibid.

52 Ibid.

53 CISA (Jointly with NSA, FBI, and others). Joint Guidance: Identifying and Mitigating Living off The Land Techniques. February 7, 2024.

54 CISA. Implementing Phishing-Resistant MFA, October 2022.

55 Meyer, L.A., Romery, S., Bertoli, G., Burt, T., Weinart, A., and Ferres, J. (Microsoft Corporation). How Effective is Multifactor Authentication in Deterring Cyberattacks? May 2022.

56 FFIEC. Authentication and Access to Financial Institution Services and Systems, August 2021.

57 CSBS. *CSBS Ransomware Self-Assessment Tool for Banks,* October 24, 2023.

58 Garrity, Patrick (VulnCheck). *"2025 Q1 Trends in Vulnerability Exploitation"*. April 24, 2025.

59 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - VI.B.3- Vulnerability and Patch Management. June 2021.

60 Ibid.

61 Ibid.

62 Ibid.

63 Ibid.

64 CISA. *CISA Insights: Remediate Vulnerabilities for Internet-Accessible Systems*.

65 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Information Security - II.C..10(d) - Patch Management. September 2016.

66 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - VI.B.3- Vulnerability and Patch Management. June 2021.

67 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Information Security - II.C..10(d) - Patch Management. September 2016.

68 CISA. CISA Insights: Remediate Vulnerabilities for Internet-Accessible Systems.

69 Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Information Security - II.C..10(d) - Patch Management. September 2016.

70 Ibid.

71 Ibid.

72 Ibid.v
(Editors). "ITL Bulletin for May 2017: Cyber-Threat Intelligence and Information Sharing". May 2017.

74 Ibid.

75 Ibid.

76 Ibid.

77 Ibid.

78 Ibid.

79 Ibid.

80 Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency. Interagency Guidance on Third-Party Relationships: Risk Management. June 2023.

81 Ibid.

82 Ibid.

83 Ibid.

84 Ibid.

CSBS

1300 I Street NW, Suite 700 East
Washington, DC 20005
202.296.2840
www.csbs.org