

**CISA Tabletop Exercise Package Financial Services Sector**

[Enter Organization Name]

<Exercise Date>

Updated June 2024

Cybersecurity and Infrastructure Security Agency

Table of Contents

[Handling Instructions………………………………………………………………………………………….……..………....3](#_Toc165986531)

[General Information 5](#_Toc165986537)

[Exercise Overview 8](#_Toc165986538)

[Module 1 9](#_Toc165986539)

[Module 2 11](#_Toc165986540)

[Appendix A: Additional Discussion Questions 13](#_Toc165986541)

[Appendix B: Case Studies 17](#_Toc165986542)

[Appendix C: Malicious Activity 19](#_Toc165986543)

[Appendix D: Contacts and Resources 21](#_Toc165986544)

[Appendix E: Acronyms 22](#_Toc165986545)

# Handling Instructions

**Delete instructions that are not applicable.**

TLP:CLEAR

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):CLEAR*”: Recipients can spread this to the world; there is no limit on disclosure. This designation is used when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. **Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.**

This document may be disseminated publicly pursuant to TLP:CLEAR and <exercise sponsor name or other authority> guidelines.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:GREEN

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):GREEN*”: Limited disclosure, recipients can spread this within their community. This designation is used when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. **Note: When “community” is not defined, assume the cybersecurity/cyber defense community.**

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:GREEN and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:AMBER

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):AMBER”:* Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. This designation is used when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:AMBER+STRICT

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as *“Traffic Light Protocol (TLP):AMBER+STRICT*: Limited disclosure, recipients can only spread this on a need-to-know basis within their organization. Note that “*TLP:AMBER+STRICT”* restricts sharing to the organization only. This designation is used when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization involved. Recipients may share TLP:AMBER+STRICT information with members of their own organization, but only on a need-to-know basis to protect their organization and prevent further harm.

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER+STRICT and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:RED

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):RED*”: For the eyes and ears of individual recipients only, no further disclosure. This designation is used when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

This document should be disseminated to applicable partners and stakeholders on a strict need-to-know basis pursuant to TLP:RED and <exercise sponsor name or other authority> guidelines due to the extreme sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

# 

# General Information

## Building Resilience

The purpose of the National Cyber Exercise Program’s (NCEP) CISA Tabletop Exercise Packages (CTEPs) is to increase your organization’s resilience by assessing and validating capabilities and identifying areas for improvement. The National Institute of Standards and Technology (NIST) defines cyber resilience as “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.”[[1]](#footnote-2)

The CTEP materials (<https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages>), including this Situation Manual, are designed to support the planning and execution of a tabletop exercise. A tabletop exercise is a discussion-based exercise in response to a scenario intended to generate a dialogue of various issues, identify strengths and areas for improvement, and/or achieve changes in perceptions about plans, policies, or procedures.[[2]](#footnote-3) NCEP also offers facilitated CTEPs. If you are interested in NCEP assistance with the planning and execution of a facilitated CTEP, please contact [cisa.exercises@cisa.dhs.gov](mailto:cisa.exercises@cisa.dhs.gov).

## Using this Situation Manual

This Situation Manual provides a scenario and accompanying discussion questions designed to identify strengths and areas for improvement, including understanding of plans, policies, and procedures. This Situation Manual is intended to be adaptable and editable.

Modules 1 and 2 contain the scenario injects and discussion questions you will use to conduct the exercise. The footnotes throughout the modules contain corresponding resources to guide your preparedness efforts, including the CISA Cross-Sector Cybersecurity Performance Goals (CPG).[[3]](#footnote-4) The appendices provide the following information to tailor the exercise discussion:

* Appendix A: Additional discussion questions that can replace or augment the existing Module 1 and 2 discussion questions.
* Appendix B: Case studies that provide real-world examples of the threats presented in this scenario.
* Appendix C: An explanation of the threats presented in this scenario.
* Appendix D: Additional cybersecurity preparedness and response resources.
* Appendix E: Reference section for acronyms used within this situation manual.

## Participant Roles and Responsibilities

**Players** have an active role in discussing or performing their primary roles and responsibilities during the exercise. Players discuss or initiate actions in response to the scenario. Players may include IT/information security personnel, emergency management personnel, human resources personnel, legal personnel, external partners, and any other personnel with a role in incident response.

**Observers** do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise. Observers may include senior-level leadership, IT/information security personnel, emergency management personnel, legal personnel, external partners, and any other personnel without a role in incident response.

**Facilitators** provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also assist with facilitation as subject matter experts during the exercise.

**Note-takers** are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

## Exercise Structure

This exercise is intended to be a multimedia, facilitated exercise. Players will participate in the following:

* Cyber threat briefing (if desired)
* Scenario modules:
  + **Module** **1:** This module introduces a compromised email from your Third-Party Service Provider (TSP) sent to your accounts payable department. Employees then lose access to cloud-based applications and systems. IT’s investigation reveals exfiltrated customer personally identifiable information (PII).
  + **Module 2:** This module introduces a ransom message on bank computer systems. Customers begin to call the bank concerned they cannot access online banking systems and national news outlets report on the ransomware attack.
* Hotwash
* ***Structure Note:*** *Modules, timeline dates, and discussion questions included in each module may be modified as desired. Additional discussion questions for each module can be found in Appendix A.*

## Exercise Guidelines

* This exercise is intended to be held in an open, no-fault environment. Varying viewpoints are expected.
* Respond to the scenario utilizing your knowledge of existing plans and capabilities, along with the valuable insights derived from your training and experience.
* Decisions are not precedent-setting and may not reflect your organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options, possible solutions, and suggested actions to resolve or mitigate a problem.
* There is no hidden agenda, and there are no trick questions. The resources and written materials provided are the basis for discussion.
* In any exercise, assumptions and artificialities are necessary to complete play within the given time, achieve training objectives, and account for logistical limitations. Please do not allow these factors to negatively impact your participation in the exercise.

## Exercise Hotwash and Evaluation

The hotwash is a short meeting held immediately after the end of the exercise discussion/conduct. The facilitator will lead participants through a review of the exercise discussion, identifying strengths and areas for improvement. The hotwash is also an opportunity for evaluators to ask clarifying questions, as needed.[[4]](#footnote-5)

# Exercise Overview

|  |  |  |
| --- | --- | --- |
| Exercise Name | Exercise Name | |
| Exercise Date, Time, and Location | Exercise Date  Time (e.g., 9:00 a.m. – 12:00 p.m.)  Exercise Location | |
| Exercise Activities | Time | Activity |
| 20 Minutes | Threat Briefing and Opening Remarks |
| 60 Minutes | Module 1 |
| 20 Minutes | Break |
| 60 Minutes | Module 2 |
| 20 Minutes | Hotwash |
| Purpose | To explore, assess, and enhance plans, procedures, and overall enterprise resilience in response to a significant cyber incident. | |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Govern, Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Discuss organizational resilience and response to cyber threats targeting the financial services sector. 2. Identify areas for improvement within processes and plans in response to a cyber incident. 3. Discuss internal and external communications plans and processes. | |
| Threat or Hazard | Cyber Attack | |
| Scenario | A TSP compromise leads to impacts to cloud-based applications and systems, online banking services, and institutional reputation. | |
| Sponsor | Exercise Sponsor | |
| Participating Organizations | Overview of organizations participating in the exercise (e.g., federal, state, local, private sector, etc.). | |
| Points of Contact (POC) | |  |  | | --- | --- | | **Insert Organization POC(s)**  Contact Information | **CISA National Cyber Exercise Program**  [cisa.exercises@cisa.dhs.gov](mailto:cisa.exercises@cisa.dhs.gov)  **Financial Services Sector Risk Management Agency**  [occip-coord@treasury.gov](mailto:occip-coord@treasury.gov) | | |

# Module 1

### Day 1

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) issue a joint alert detailing the tactics, techniques, and procedures of a threat actor targeting TSPs who service U.S. based financial institutions.[[5]](#footnote-6) The threat actor used spear phishing tactics against TSPs to gain credentials and used these credentials to access the TSPs’ customer data. To date, there are confirmed incidents impacting multiple financial institutions, including credit unions and community banks, whose data was stolen from their TSP(s).

## Discussion Questions

Discussion questions included in each module are designed to explore different aspects of your cyber resilience. The questions may be modified as desired. Additional questions can be found in Appendix A.

1. What are the greatest cyber threats to your organization?
   1. What are the possible impacts of an intrusion into your systems?
2. What cybersecurity threat information does your organization receive?
   1. What are your primary sources of information?
   2. How do you determine what information is relevant to your equipment and operations?
   3. What threat information is most useful?
   4. What actions would your organization take in response to an alert like the one presented in the scenario?
3. Discuss your organization’s cyber resilience planning.
   1. Does your organization apply Zero Trust Architecture (ZTA)/zero-trust concepts?[[6]](#footnote-7)
4. Has your organization conducted a risk assessment to identify specific cyber threats, vulnerabilities, and critical assets?
   1. What improvements were implemented to enhance cyber resilience following recent risk assessments?

### Day 6

Your accounts payable department receives an email appearing to be from your TSP. The email states the TSP’s billing software is offline in order to perform an update. The most recent invoice will not be available through the online payment portal, and the invoices will be emailed instead.[[7]](#footnote-8) Later that day, accounts payable receives another email with a PDF attachment. Accounts payable personnel attempted to open the file, but it appears to be corrupt and cannot be opened. When accounts payable reaches out to your TSP, the TSP states they did not email the invoices, and the online payment portal is functional.

1. Describe your organization’s cybersecurity training program for employees.
   1. How often are employees required to complete this training?
   2. What additional training is required for employees who have system administrator-level privileges?
   3. What type of training methods or approaches have you found most beneficial?
2. What is the role of cybersecurity in the review and selection of TSP support?
   1. What cybersecurity language (e.g., cybersecurity training and cyber incident notification requirements) is included within TSP contracts?
   2. How do you evaluate the cybersecurity posture of your vendors?
   3. How often are contracts reviewed?
3. What level of access do your TSP have to your organization’s network?[[8]](#footnote-9)
   1. How often are TSP access rights and data logs reviewed?

### Day 7

Employees contact your information technology (IT) help desk stating they are unable to access any cloud-based applications and systems. While investigating the issue, your IT department discovers small amounts of customer data was exfiltrated from cloud storage.

1. How is your network configured (e.g., network segmentation, least privilege access, etc.) to defend against malicious actors?
2. How does your organization baseline network activity?
   1. How do you distinguish between normal and abnormal traffic?
   2. What are your next steps when abnormal activity is detected/reported?
   3. What intelligence feeds for indicators of compromise does your organization use?
3. What IT systems or processes are the most critical to your organization?
4. How would you coordinate with your cloud service provider to investigate anomalies with cloud-based services?

### Day 8

Your IT department discovers significant customer data exfiltration after investigating system access issues.[[9]](#footnote-10)

1. What steps do you take to ensure organizational data is secure from data loss/theft?

# Module 2

### Day 9 - Morning

Computers throughout the organization reboot. A ransom note appears on screens stating full access to systems and functionality will be restored for $5 million in cryptocurrency. Your organization’s internal-facing systems are unavailable. Additionally, online banking services, such as bill pay and funds transfer, are unavailable for customers.

## Discussion Questions

1. Using your organization’s Cyber Incident Response Plan (CIRP)/incident response/continuity of operations plan, describe the actions your organization would take to minimize impact on current operations.
   1. How does your plan define escalation criteria, notifications, activations, and/or courses of action?
   2. What guidance does the plan include on assessing the severity of the incident?
   3. How does incident severity level dictate response actions?
   4. How are critical systems and processes incorporated within your plan?
2. Explain your organization’s decision-making process regarding ransomware payment.[[10]](#footnote-11)
   1. Are ransomware policies/procedures included in your CIRP?

### Day 9 – Afternoon

Your customer service department is overrun with phone calls from customers demanding answers to why they cannot access online banking services. When customer service representatives are unable to assist with account functions and adequately answer questions, customers demand to withdraw money from their accounts.

1. Are you able to continue to provide services to your customers while responding to this incident?
   1. What alternative systems or manual processes are implemented to continue operations if a critical system is unavailable for a significant period?
   2. Who can authorize the use of alternate systems or procedures?
   3. How long can you operate using manual processes or alternate systems when your primary critical systems fail?
   4. What additional staffing requirements are necessary for alternate systems or procedures?
2. What incident-related information are you sharing with customer-facing employees?

### Day 9 – Evening

National news outlets report other financial institutions in your region are unable to provide banking services to customers. Multiple media organizations contact your financial institution for comment.[[11]](#footnote-12)

1. What incident-related information are you sharing externally (e.g., with customers, partners)?
   1. How do you respond to the media inquiries?
2. What legal and regulatory notifications are required based on the scenario?
3. When are notifications made?
4. Who is responsible for making the notifications?
5. How are TSP vendors involved in your incident response?
   1. Is this documented in your CIRP?

### Day 10

The news of the attacks and lack of access to banking services across the region leads to widespread attempts to withdraw funds and close accounts at your financial institution as well as other financial institutions in the region.

1. How sufficient are your organization’s current internal resources for responding to the cyber incidents in this scenario?
   1. What additional resources outside of your organization are necessary for responding to the cyber incident?
   2. What are the processes or procedures for requesting additional resources?
   3. What external partners (e.g., Department of the Treasury, CISA, FBI, vendors) would you contact for assistance?
2. How would you work to regain public trust and the trust of your customers following this incident?
3. Based on discussion and lessons learned, what changes will you implement to increase the resilience of your organization?

# 

# Appendix A: Additional Discussion Questions

The following section includes supplemental organizational resilience discussion questions designed to guide exercise play. Questions are aligned with the NIST functional areas and organizational roles and responsibilities. Exercise planners are encouraged to select additional, applicable discussion questions for the chosen scenario to bolster participant conversation. ***This instructional paragraph, as well as undesired discussion questions, should be deleted.***

## Cyber Resilience

1. What additional cybersecurity features, such as multi-factor authentication (MFA) or access controls, can your organization implement to increase organizational resilience?
2. How is defense-in-depth incorporated into your organizational system/network security?
   1. Are there any areas where defense-in-depth practices could be strengthened?
3. Discuss how cyber preparedness is integrated with your current all-hazards preparedness efforts.
4. Describe your organization’s patch management and vulnerability management plans.
   1. Describe your policies on remote access to your organization’s network.
   2. What security protocols (MFA, encryption, etc.) exist on your hardware?
5. How often are your cybersecurity plans, policies, and procedures externally reviewed or audited?
   1. What were the most recent results and action items that followed?
6. Discuss your risk management strategy.
7. How is it developed/maintained?
8. What considerations are addressed in your risk management strategy (e.g., extended downtime, impaired functionality, loss of data, etc.)?
9. Describe the relationship between the IT risk management strategy and the enterprise risk management strategy.
10. What are the cybersecurity objectives for your organization?
    1. How do these align with your business objectives?
11. Describe your organization’s review process for your cyber incident response plan (CIRP).
12. How is your CIRP integrated with other incident or emergency response/management plans?
13. How often is the CIRP reviewed?
14. Which individual(s) and department(s) are responsible for reviewing and updating the plan?
15. How are updates to the plan communicated to department or agency employees?
16. How is the integrity of your critical data protected and validated?
17. What external entities have access to your data?
18. How would those entities report a breach of their systems to your office?

## Accounts & Privileges

1. What are your organization’s policies or procedures for IT account management?
2. What are the protocols for establishing, activating, modifying, disabling, and removing accounts?
3. Describe your organization’s bring your own device (BYOD) policy.
4. Describe your organization’s employee off-boarding process.
5. Is this process coordinated with IT and Human Resources (HR)?
6. What additional actions are taken if the employee’s termination is contentious?
7. How does your organization retrieve all information system-related property during the employment termination process (e.g., authentication token, system administrator’s handbook/manual, keys, identification cards, etc.)?

## Incident Identification

1. How are cyber incidents reported within your organization?
2. What would trigger the reporting requirements established by regulation, state law, and/or organization policy?
3. What training do employees receive regarding reporting requirements and your cyber incident response plan?
4. What cybersecurity incident escalation criteria is defined in your cyber incident response plan?
5. Who is responsible and what actions would they take based on the scenario?
6. Who should be notified internally and externally according to the plan?
7. When would leadership be notified?
8. Discuss your organization’s intrusion detection capabilities and analytics that alert you to a potential cyber incident.
9. What type of hardware and/or software does your organization use to detect and prevent malicious activity on your systems/network?
10. How often is your organization’s data reviewed?
11. How would you determine whether unauthorized manipulation of data occurred?

## Incident Response

1. What essential functions are impacted by the incidents described in the scenario?
2. If primary communications are compromised, how do you provide information to internal and external entities?
3. What are your processes for collecting evidence and maintaining the chain of custody during a cyber incident?
4. At what point in the scenario would you contact law enforcement?
   1. How would a law enforcement investigation impact containment, eradication, and recovery efforts?
5. What are the processes for contacting critical personnel outside of core hours?
6. How do you proceed if critical personnel are unreachable or unavailable?
7. How would a breach of vendor(s) affect your organization if they have access to your information?
8. What are the notification requirements to your organization for breaches?

## Recovery

* 1. When does your organization determine a cyber incident is resolved?

1. Who makes this decision?
2. What post-incident activities would your organization conduct?
   1. What actions would your organization take if your IT/incident response staff could not confirm the integrity of your systems/data?
3. What is the risk associated with reactivating critical business processes and systems?
4. Describe the process to completely rebuild these systems.
5. What factors do you consider when making these decisions?

## Training & Exercises

1. What training does your cybersecurity incident response team undergo to detect, analyze, and report malicious activity?
2. What additional training and/or exercise requirements do you require for your incident response staff?
3. How often does your organization exercise its CIRP?
4. Who is involved in the exercises?
5. What external agencies are involved in the exercises?
6. How do your organization’s training and exercise efforts address both physical and cyber risks?
7. How often do senior staff/leadership participate in cybersecurity exercises?

## Senior Leaders

1. As a leader in your organization, what cybersecurity resilience goals have you set?
2. How do these goals align with organizational objectives?
3. Describe your organization’s cybersecurity culture.
4. What cybersecurity training is required for senior leadership?
5. At what point would you activate your organization’s Security Operations Center (SOC)/Emergency Operations Center (EOC)?
6. What is your role during a cyber incident?
7. What information do you need to support your decision-making process?
8. What are the gaps in your cybersecurity workforce?
9. How does your organization recruit, develop, and retain cybersecurity staff?

## Public Information

* + - 1. What training do employees receive on reporting contact with the media?
      2. How do you build and maintain trust with the public?

## Legal

1. Describe the role your legal office/department plays in responding to a cyber incident.
   1. How does your legal team contribute to the incident management and recovery process?
2. Does your legal office/department create or maintain documents to assist with responding to a cyber incident?
   1. What documents might your legal office anticipate preparing or reviewing during such incidents?

# Appendix B: Case Studies

## Attack Against Cloud Service Provider Impacts Credit Unions

On November 26, 2023, a cloud service provider (CSP) owned by a credit union-focused technology firm that serves U.S. credit unions fell victim to a ransomware attack. The attack impacted approximately 60 CSP customers. The ransomware attack against the CSP resulted in service outages across customer credit unions.

The cloud service provider notified impacted credit unions, confirmed that some of their data was compromised and offered to provide credit monitoring and identity restoration services to any impacted individuals.[[12]](#footnote-13),[[13]](#footnote-14) The National Credit Union Administration confirmed affected credit unions were fully operational over two weeks after the CSP confirmed their network was compromised. The NCUA noted the impacted credit unions’ members’ funds were safe, and members had access to their funds.[[14]](#footnote-15)

## Large U.S. Bank Suffers Multiple Data Breaches

A large U.S. financial institution suffered three significant data breaches in the span of approximately three and a half years. The most recent data breach, in May 2023, was the result of a supply chain compromise. Previously undisclosed vulnerabilities in a third-party file transfer software, which was used by the bank’s payment processing and mobile banking services provider, allowed threat actors to access customer data. The customer and employee data stolen included names, addresses, phone numbers, tax records, and social security numbers. The financial institution sent a notice to customers and provided credit monitoring, fraud consultation, and identity theft restoration for two years.[[15]](#footnote-16) This data breach did not compromise the bank’s internal IT systems or disrupt banking operations; the data was accessed via the compromised vendor who utilized the file transfer software.[[16]](#footnote-17)

In June 2022, the financial institution reported a data breach impacting over 1.5 million customers.[[17]](#footnote-18) The breach involved access to the financial institution’s corporate network by an unauthorized party, resulting in the theft of sensitive customer information, including Social Security numbers, banking details, and other personal data such as names, addresses, and birthdates.[[18]](#footnote-19) The breach occurred in December 2021 and was disclosed in June 2022. The financial institution notified affected individuals through postal mail and offered two years of free identity monitoring services as a precautionary measure.

Cyber Incident Against Debt Collector Leads to Theft of Client Data

In February 2023, a debt collection company whose customers included major U.S. financial institutions fell victim to a cyber incident resulting in a data breach. The threat actors gained access to customer information databases that included over a million individuals.[[19]](#footnote-20) The debt collection company was not aware its networks were infiltrated for approximately three days. The threat actors stole customer information, including names, addresses, Social Security numbers, financial account numbers, credit and debit card numbers, and the security codes/passwords associated with the accounts. The debt collection company reported a data breach to regulators in multiple states, declaring they “obtained assurances that the unauthorized third-party no longer has access to any data.”[[20]](#footnote-21) The company offered free identity theft monitoring services for two years for affected customers.[[21]](#footnote-22)

# Appendix C: Malicious Activity

## Social Engineering and Phishing

One of the most prominent tactics cyber threat actors use to exploit network and system vulnerabilities is social engineering, the manipulation of users through human interaction and the formation of trust and confidence to compromise information or download files. Common social engineering techniques involves the use of phishing, vishing, and smishing. Phishing uses email and/or malicious websites to solicit personal information or to trick individuals into downloading malicious software. Vishing uses voice communication to convince a victim to share sensitive information. Advanced vishing incidents can take place completely over voice communications by exploiting Voice over Internet Protocol (VoIP) solutions and broadcasting services. VoIP easily allows caller identity to be spoofed. Smishing uses SMS/text messages to send malicious links, email addresses, and phone numbers.

Social engineering is effective for compromising networks, and evading intrusion detection systems without leaving a log trail. While technical exploits aim to bypass security software, social engineering exploits are more difficult to guard against due to the human factor. Organizations should take steps towards strengthening employee cybersecurity awareness training, including training personnel to be cautious of suspicious emails, providing instruction on where to forward them, and keeping software and systems up to date. Organizations can also implement software designed to safeguard sensitive information, detect unsafe URLs, block phishing websites, detect known phishing and malware, and implement MFA to guard against the use of stolen credentials.

### Additional Resources

* Avoiding Social Engineering and Phishing Attacks

(<https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks>)

* Phishing Guidance: Stopping the Attack Cycle at Phase One (<https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one>)

## Ransomware

Ransomware is a type of malicious software designed to deny access to victims’ data or systems through encryption with a key only known by the malicious actor who deployed the malware. Once encrypted, the ransomware directs the victim to pay the attacker, typically in the form of cryptocurrency. Ransomware typically spreads through phishing emails or by users unknowingly visiting an infected website. Ransomware and associated data breach incidents can severely impact business processes, leaving organizations unable to access data necessary to function. The economic and reputational impacts of ransomware and data extortion have proven challenging and costly for organizations of all sizes throughout the initial disruption and, at times, extended recovery. Recovery can be an arduous process and there is no guarantee the victim will receive access to their data or systems if the ransom is paid. For more information on best practices to protect users from the threat of ransomware, as well as recent Alerts on specific ransomware threats, see the resource list below.

### Additional Resources

* CISA Stop Ransomware Website (<https://www.cisa.gov/stopransomware>)
* CISA Stop Ransomware Guide (<https://www.cisa.gov/resources-tools/resources/stopransomware-guide>)
* Protecting Against Ransomware (<https://www.cisa.gov/news-events/news/protecting-against-ransomware>)
* Financial Crimes Enforcement Network (FinCEN) Combats Ransomware (<https://www.fincen.gov/fincen-combats-ransomware>)

# Appendix D: Contacts and Resources

Federal Government Contacts

* CISA (contact: [central@cisa.gov](mailto:central@cisa.gov), <https://www.cisa.gov>)
* United States Secret Service (USSS) Field Offices and Electronic Crimes Task Forces (ECTFs) (contact: <https://www.secretservice.gov/contact/field-offices>, <https://www.secretservice.gov/investigation/cyber>)
* Federal Bureau of Investigation (FBI)
* Field Offices (contact: <https://www.fbi.gov/contact-us/field-offices>)
* Internet Crime Complain Center (IC3) (contact: [http://www.ic3.gov](http://www.ic3.gov/))
* National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center (contact: [cywatch@ic.fbi.gov](mailto:cywatch@ic.fbi.gov); 855-292-3937)

Financial Services Sector Resources

* CISA Financial Services Sector (<https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/financial-services-sector>)
* U.S. Department of the Treasury Financial Institutions (<https://home.treasury.gov/about/offices/domestic-finance/financial-institutions>)
* FinCEN Alerts/Advisories/Notices/Bulletins/Fact Sheets (<https://www.fincen.gov/resources/advisoriesbulletinsfact-sheets>)
* National Credit Union Administration Cybersecurity Resources (<https://ncua.gov/regulation-supervision/regulatory-compliance-resources/cybersecurity-resources>)
* Financial Services Information Sharing and Analysis Center (<https://www.fsisac.com/>)

Preparedness Resources

* CISA Find Help Locally (<https://www.cisa.gov/audiences/find-help-locally>)
* CISA Cross-sector Cybersecurity Performance Goals (<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>)
* NIST Cybersecurity Framework Tools ([<https://www.nist.gov/cyberframework>](https://www.nist.gov/cyberframework))

State Level Resources

* DHS Fusion Centers (<https://www.dhs.gov/state-and-major-urban-area-fusion-centers>)

Additional Resources

* Cybersecurity & Information Systems Information Analysis Center (<https://csiac.org/>)
* InfraGard (<https://www.infragard.org/Files/InfraGard_Redesign_2-24-2022.pdf>)
* Internet Security Alliance (<https://isalliance.org/>)
* International Association of Certified Information Sharing and Analysis Organizations ([http://www.certifiedisao.org](http://www.certifiedisao.org/); contact: [operations@certifiedisao.org](mailto:operations@certifiedisao.org))
* National Council of Information Sharing and Analysis Centers ([https://www.nationalisacs.org](https://www.nationalisacs.org/))

# Appendix E: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| BYOD | Bring Your Own Device |
| CIRP | Cyber Incident Response Plan |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CPG | Cybersecurity Performance Goals |
| CSF | Cybersecurity Function |
| CSP | Cloud Service Provider |
| CTEP | CISA Tabletop Exercise Package |
| FBI | Federal Bureau of Investigation |
| FinCEN | Financial Crimes Enforcement Network |
| HR | Human Resources |
| IOC | Indicators of Compromise |
| IP | Internet Protocol |
| IT | Information Technology |
| MFA | Multi Factor Authentication |
| NCEP | National Cyber Exercise Program |
| NIST | National Institute of Standards and Technology |
| OT | Operational Technology |
| POC | Point of Contact |
| TLP | Traffic Light Protocol |
| TSP | Third-Party Service Provider |
| VoIP | Voice over Internet Protocol |
| ZTA | Zero Trust Architecture |

1. “Computer Security Resource Center Glossary: Cyber Resilience,” National Institute of Standards and Technology, accessed August 2, 2023, <https://csrc.nist.gov/glossary/term/cyber_resiliency>. [↑](#footnote-ref-2)
2. “Homeland Security Exercise and Evaluation Program,” FEMA, February 2020, <https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep>. [↑](#footnote-ref-3)
3. This document does not intend to map directly to any regulatory requirements to which members of this sector may be subject, nor is it intending to suggest that compliance with the CPGs would be sufficient to meet any such regulatory requirements. [↑](#footnote-ref-4)
4. FEMA, “Homeland Security Exercise and Evaluation Program,” January 2020, <https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep>. [↑](#footnote-ref-5)
5. CISA Cybersecurity Alerts & Advisories, <https://www.cisa.gov/news-events/cybersecurity-advisories> [↑](#footnote-ref-6)
6. CISA Resources, “Zero Trust Maturity Model,” <https://www.cisa.gov/zero-trust-maturity-model> [↑](#footnote-ref-7)
7. NIST CPRT - CSF 2.0, “PR.AT-01 – Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.AT-01> [↑](#footnote-ref-8)
8. NIST CPRT – CSF 2.0, “GV.SC – Govern; Cybersecurity Supply Chain Risk Management,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=GV.SC> [↑](#footnote-ref-9)
9. NIST CPRT – CSF 2.0, “RS.MA-02: Incident reports are triaged and validated,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RS.MA-02> [↑](#footnote-ref-10)
10. CISA, “Stop Ransomware,” <https://www.cisa.gov/stopransomware> [↑](#footnote-ref-11)
11. NIST CPRT – CSF 2.0, “RS.CO: Incident Response Reporting and Communication,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RS.CO> [↑](#footnote-ref-12)
12. Matt Kapko, “Credit Unions Recover from Outages Caused by Third-Party Ransomware Attack,” Cybersecurity Dive, December 14, 2023, [https://www.cybersecuritydive.com/news/credit-unions-recover-third-party-ransomware/702540/](https://urldefense.us/v3/__https:/www.cybersecuritydive.com/news/credit-unions-recover-third-party-ransomware/702540/__;!!BClRuOV5cvtbuNI!Cxs4_mwcit9KFhsIar7K0tUT4S7Pgs1QaKffbeqn0ToMwnuhkDjkVBns9BfJz3_MIV1CHo0xINeucXH2S-SRcIDoAjlnsAvs3Hw$). [↑](#footnote-ref-13)
13. Jonathan Greig, “60 Credit Unions Facing Outages Due to Ransomware Attack on Popular Tech Provider,” *The Record*, December 1, 2023, <https://therecord.media/credit-unions-facing-outages-due-to-ransomware>. [↑](#footnote-ref-14)
14. Kapko, ibid. [↑](#footnote-ref-15)
15. Alessandro Mascellino, “Flagstar Bank MOVEit Breach Affects 800K Customer Records,” *Infosecurity Magazine,* October 10, 2023, <https://www.infosecurity-magazine.com/news/flagstar-bank-moveit-breach/>. [↑](#footnote-ref-16)
16. Alicia Hope, “Flagstar Bank Suffers a MOVEit Data Breach Impacting over 800,000 Customers,” *CPO Magazine,* October 18, 2023, <https://www.cpomagazine.com/cyber-security/flagstar-bank-suffers-a-moveit-data-breach-impacting-over-800000-customers/>. [↑](#footnote-ref-17)
17. Office of the Maine Attorney General, “Data Breach Notifications,” 6/17/2022, <https://apps.web.maine.gov/online/aeviewer/ME/40/667f2112-b49f-445d-be03-dee38e32bf8e.shtml>. [↑](#footnote-ref-18)
18. New Hampshire Department of Justice, “Flagstar Bank,” June 21, 2022, <https://mm.nh.gov/files/uploads/doj/remote-docs/flagstar-bank-20220621.pdf>. [↑](#footnote-ref-19)
19. Sead Fadilpasic, “Data breach at US debt collector exposes over a million users,” *TechRadar*, May 25, 2023, <https://www.techradar.com/news/data-breach-at-us-debt-collector-exposes-over-a-million-users>. [↑](#footnote-ref-20)
20. Jonathan Greig, “Capitol One Becomes Latest Bank Affected by Cyberattack on Debt-Buying Giant,” *The Record,* June 23, 2023, <https://therecord.media/capital-one-ncb-management-services-data-breach>. [↑](#footnote-ref-21)
21. Console and Associates, P.C., “Third-Party Data Breach at NCB Management Services Affects 15,549 TD Bank Customers,” *JDSupra*, May 15, 2023, <https://www.jdsupra.com/legalnews/third-party-data-breach-at-ncb-8346941/>. [↑](#footnote-ref-22)