

**[Enter Organization Name]**

**CISA Tabletop Exercise Package**

**Insider Threat**

## <Insert Date>

## Cybersecurity and Infrastructure Security Agency

Updated September 2023

Table of Contents

[Handling Instructions 3](#_Toc143257613)

[Exercise Overview 5](#_Toc143257619)

[General Information 6](#_Toc143257620)

[Module 1 8](#_Toc143257621)

[Module 2 10](#_Toc143257622)

[Appendix A: Additional Discussion Questions 13](#_Toc143257623)

[Appendix B: Acronyms 16](#_Toc143257624)

[Appendix C: Case Studies 17](#_Toc143257625)

[Appendix D: Attacks and Threats 18](#_Toc143257626)

[Appendix E: Contacts and Resources 20](#_Toc143257627)

# 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>.

# 

# 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 | Examine the cyber resilience of <Organization> in response to an insider-based cyber incident. | |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Evaluate <Organization’s> supply chain-oriented threats and the impact on organizational cyber resilience. 2. Discuss <Organization’s> risk and vulnerabilities associated with malicious and unmalicious insider threats. 3. Identify areas of improvement in cyber incident response plans and overall organizational resilience during and following a significant cyber incident. | |
| Threat or Hazard | Insider Threat – Cyber | |
| Scenario | A disgruntled former employee takes advantage of their new position at one of your third-party vendors to exploit vulnerabilities in your systems created by a supply chain issue. An error by another employee discloses personally identifiable information (PII). | |
| Sponsor | Exercise Sponsor | |
| Participating Organizations | Overview of organizations participating in the exercise (e.g., federal, state, local, private sector, etc.). | |
| Points of Contact | |  |  | | --- | --- | | **Insert Organization POC(s)**  Contact Information | **CISA National Cyber Exercise Program (NCEP)**  [cisa.exercises@cisa.dhs.gov](mailto:cisa.exercises@cisa.dhs.gov) | | |

# General Information

## Building Resilience

The purpose of the National Cyber Exercise Program’s CISA Tabletop Exercise Packages (CTEPs) is to increase your organization’s cyber resilience 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)

## Using this Situation Manual

Modules 1 and 2 contain the scenario injects and discussion questions you will use to conduct the exercise. There are footnotes with corresponding resources throughout the modules to guide your preparedness efforts. 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: Reference section for acronyms used within this situation manual.
* Appendix C: Case studies that provide real-world examples of the threats presented in this scenario.
* Appendix D: An explanation of the threats presented in this scenario.
* Appendix E: Additional cybersecurity preparedness and response resources.

## 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.

**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.

**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 microprocessor vulnerability requiring an expensive replacement process, an employee email inadvertently discloses personally identifiable information, and a disgruntled employee who threatens the organization.
  + **Module 2:** This module presents an unknown attacker exploiting the vulnerability identified in Module 1 and the loss of critical files and data.
* 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 facilitator will lead a hotwash with participants at the end of the exercise to address any ideas or issues that emerge from the exercise discussions.

# Module 1

### Day 1

The Cybersecurity and Infrastructure Security Agency (CISA) releases an alert[[2]](#footnote-3) with details on the Common Vulnerabilities and Exposures (CVEs) that are routinely and frequently exploited by malicious cyber actors.[[3]](#footnote-4) Your information technology (IT) department identifies a vulnerability in a type of microprocessor that is widely deployed within your organization, which may grant an attacker access to sensitive data.

### Day 2

After investigating the vulnerability, your IT department determines that it is necessary to replace the impacted microprocessor. Due to the expense and time needed to replace the impacted microprocessors, it is determined that a year-long roll out and update strategy is required.

### Day 8

At the end of a long workday, one of your employees inadvertently sends an email containing PII from <your organization, customers, clients, etc.> to several external contacts.[[4]](#footnote-5)

### Day 9: Morning

The PII disclosure is discussed during the morning meeting. A representative from a key department loudly berates another team member about the PII breach. Their behavior is far outside your organization’s definition of acceptable conduct. This representative, though highly competent in their field, has engaged in similar behavior in the past and had been formally cautioned by Human Resources that any future instances of such conduct would result in termination.

### Day 9: Afternoon

Senior management makes the decision to terminate the employee due to their unprofessional conduct. They react poorly to the notification, screaming expletives at senior management and warning them that “You will be sorry!” for firing them.[[5]](#footnote-6)

## Discussion Questions

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

1. What are the greatest cybersecurity threats to your organization?
2. What cybersecurity threat information does your organization receive?
   1. What cyber threat information is most useful?
   2. How is information disseminated across your organization and by whom?
   3. What actions would your organization take following an alert like the one presented in the scenario?
3. Has your organization conducted a risk assessment to identify specific cyber threats, vulnerabilities, and critical assets?
   1. What information technology (IT) systems or processes are the most critical to your organization?
   2. Describe your organization’s asset management plan and how you prioritize critical assets.
   3. What improvements have been implemented to enhance cyber resilience following recent risk assessments?
   4. Does your organization have a vulnerability management program dedicated to mitigating known exploited vulnerabilities in internet-facing systems?
4. How does your organization mitigate insider threats? Does your organization have an insider threat management program?
   1. What are some behavioral indicators of an insider threat?
   2. What type of training do employees at your organization receive on identifying a potential insider threat?
5. Describe your organization’s cybersecurity training program for employees.
   1. How often are employees required to complete this training?
   2. Is training required during employee onboarding before granting system/network access?
   3. What additional training is required for employees who have system administrator-level privileges?
   4. What type of training methods or approaches have you found most beneficial?
6. How does your organization prevent the disclosure of PII?
7. What are your organization’s processes and procedures to revoke system access when an employee resigns or is terminated?
   1. Are there any additional processes implemented if the employee’s termination is contentious?
   2. Does your organization retrieve all information system-related property (e.g., authentication key, system administration's handbook/manual, keys, identification cards, etc.) during the employment termination/off boarding process?

# Module 2

### Day 13

Staff begins the process of replacing impacted microprocessor chips. Due to high demand for replacement materials, the estimated process will take 18 months to complete.

### Day 23

During a meeting with a key vendor, it is revealed that they have hired your recently terminated employee.[[6]](#footnote-7) The vendor assures your representatives that the employee will not attend any meetings with your organization.

### Day 42

Several employees contact the help desk with complaints of difficulties accessing information on shared network drives. Some files appear to have been renamed, moved, or deleted. The IT department can recover the missing files from backups, but any work completed following the creation of the latest backup has been lost.[[7]](#footnote-8)

### Day 43: Morning

The IT department reviews logs to determine the issue with the files.[[8]](#footnote-9) They quickly identify the presence of an unauthorized administrator-level accoun. The account is immediately deactivated.

### Day 43: Afternoon

The IT department determines the unknown administrator account was added to the system by exploiting the microprocessor vulnerability.[[9]](#footnote-10) After accessing the memory of the machine, the attacker was able to obtain an administrator password used to install a recent security patch, create a new administrator account, and move laterally through the system.[[10]](#footnote-11)

### Day 44: Morning

The IT department determines that the Internet Protocol address used to create the unauthorized administrative account belongs to your third-party vendor.[[11]](#footnote-12)

### Day 44: Afternoon

Staff is frantically calling your support desk. Files crucial to your organization’s ability to complete its core functions appear to have been deleted.[[12]](#footnote-13)

## Discussion Questions

1. Discuss your organization’s cyber resilience planning.
   1. What IT infrastructure has been identified to support mission essential functions in continuity of operations and incident response plans?
   2. How has your organization prioritized IT infrastructure for restoration?
   3. How has cybersecurity been integrated into your continuity plans?
2. Does your organization have backups of vital records stored in a location separate from your primary working files/copies?
3. How frequently do you run backups?
4. How long do you keep copies of archived files backed up?
5. How long would it take to restore primary files from backups?
6. Utilizing your organization’s cyber incident response plan (CIRP), describe the actions that your organization would take at this time.
   1. What CIRP training do you provide your employees?
   2. What guidance does the CIRP include on assessing the severity of the incident?
   3. How does incident severity level determine response?[[13]](#footnote-14)
7. What are your organization’s policies or procedures for IT account management?
8. What are the protocols/proceedures for establishing, activating, modifying, disabling, and removing accounts?
9. Do these policies or procedures include protocols/steps for notifying IT account managers/administrators when users are terminated or resign?
10. How would you respond to the discovery of an unauthorized administrator account on your systems?
11. What capabilities and resources are required to respond to this scenario? [[14]](#footnote-15)
12. What additional resources outside of your organization are necessary for responding to the cyber incident?
13. What are the processes or procedures for requesting additional resources?
14. What external partners (e.g., CISA, FBI, etc.) would you contact for assistance?
15. How does your organization determine account access for personnel?
    1. How is unauthorized access monitored?
    2. Describe the process for changing or revoking account access, if needed?
16. What alternative systems or manual processes are implemented to continue operations if a critical system is unavailable for a significant period?
17. Who can authorize use of alternate systems or procedures?
18. How long can you perform manual or alternate processes on your critical systems?
19. At what point in the scenario would you contact law enforcement?[[15]](#footnote-16)
    1. How would relationships with law enforcement and other partners be managed?
    2. Is this process documented in your CIRP?
    3. Are processes and resources in place for evidence preservation and collection?
20. Based on discussion, 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 page, as well as undesired discussion questions, should be deleted.*

## Cyber Resilience

1. Discuss how cyber preparedness is integrated into your current all-hazards preparedness efforts.
2. 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?
3. Describe your <organization>’s review process for your CIRP.
4. How often is the CIRP reviewed?
5. Which individual(s) and department(s) are responsible for reviewing and updating the plan?
6. How are updates to the plan communicated to relevant employees?
7. Discuss your supply chain concerns related to cybersecurity infrastructure.
8. Describe your patch management plan.
9. What risk assessments have been performed on network servers?
10. What processes are in place to proactively evaluate each server’s criticality and applicability to software patches?
11. What considerations (e.g., extended downtime, loss of data, impaired functionality, etc.) are addressed in the plan’s risk management strategy?
12. What is your method for tracking and identifying firmware vulnerabilities in your network?
13. How are IT and business continuity functions coordinated with physical security?[[16]](#footnote-17)
14. What processes do you have to ensure that your external dependencies (e.g., contractors, power, water, etc.) are integrated into your security and continuity planning programs?
15. How is the integrity of your critical data protected and validated?
16. What external entities have access to the database?
17. How would those entities report a breach of their systems to your office?
18. What mission essential functions are impacted by the incidents described in the scenario?
19. How does your organization maintain availability of key assets (e.g., network connectivity, etc.)?
20. What policies and procedures does <your organization> use to decide when and how to restore backed-up data?
    1. How does <your organization> incorporate measures for ensuring the integrity of backup data before restoration?

## Accounts & Privileges

1. Describe <your organization>’s bring your own device (BYOD) policy.

## Incident Identification

1. How are cyber incidents reported within <your organization>?
2. What would trigger the reporting requirements established by regulation, law, and/or organization policy?
3. What training have employees received regarding reporting requirements and your CIRP?
4. What cybersecurity incident escalation criteria are defined in your CIRP?
5. Who is responsible and what actions would they take based on the scenario?
6. Who needs to be notified internally and externally according to the plan?
7. When is leadership 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? How would you determine whether unauthorized manipulation of data has occurred?

## Incident Response

1. What are your processes for collecting evidence and maintaining the chain of custody[[17]](#footnote-18) during a cyber incident?
2. How would a breach of <vendor> affect <your organization> if they have access to your information?
3. What are the notification requirements to <your organization> for breaches?

## Recovery

1. When does <your organization> determine a cyber incident is over?
2. Who makes this decision?
3. What post-incident activities would your organization conduct?
4. What actions would <your organization> take if your IT/incident response staff could not confirm the integrity of your systems/data?
5. What is the risk associated with reactivating critical business processes and systems?
6. How long and costly is the process to completely rebuild these systems?
7. 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 exercise?
5. How do your organization’s training and exercise efforts address both physical and cyber risks?
   1. Have senior staff participated in a cybersecurity exercise?

## Senior Leaders

1. As a leader in your organization what cybersecurity resilience goals have you set?
2. What cybersecurity training is required for senior leadership?
3. What is your role during a cyber incident?
4. What information do you need to support your decision-making process?
5. What are the gaps in your cybersecurity workforce?
6. How does your your organization recruit, develop, and retain cybersecurity staff?

## Public Information

* + - 1. What training is provided to employees regarding reporting any contact with the media to the appropriate public information personnel?
      2. How do you build and maintain trust with the public?

## Legal

1. What is the role of the legal department during a cyber incident?
2. What issues need to be addressed based on the scenario?
3. What legal documentation should your organization have for cyber incidents?

# Appendix B: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| CIRP | Cyber Incident Response Plan |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CPG | Cybersecurity Performance Goals |
| CSF | Cybersecurity Framework |
| BYOD | Bring Your Own Device |
| DHS | U.S. Department of Homeland Security |
| FBI | Federal Bureau of Investigation |
| IT | Information Technology |
| MOU/MOA | Memorandum of Understanding/Memorandum of Agreement |
| NIST | National Institute of Standards and Technology |
| PII | Personally Identifiable Information |
| TLP | Traffic Light Protocol |
| ZTA | Zero Trust Architecture |

# Appendix C: Case Studies

## Sensitive Client Information Stolen by Insider

The parent company of a mobile payment application (app), reported a data breach of the app’s client information in early December 2021. A former employee accessed and downloaded sensitive customer financial data after leaving the company. The stolen data included customer names, brokerage account numbers, brokerage portfolio values and holdings, and stock trading information.[[18]](#footnote-19) The payment app notified law enforcement and conducted a forensic investigation to address the issue, emphasizing that company policy states employees’ access is revoked upon leaving the company. A total of 8.2 million current and former clients were notified of the incident.[[19]](#footnote-20)

Inside Hacker Accesses Customer Credentials and Applications

A software engineer for the cloud hosting company contracted by a major financial company to provide cloud based services was accused of infiltrating a company server and obtaining access to 140,000 Social Security numbers, 1 million Canadian Social Insurance numbers, and 80,000 bank account numbers, along with customers’ personal financial information. The software engineer exploited a misconfigured web firewall to gain entry.[[20]](#footnote-21)

The software engineer did not attempt to remain anonymous; they posted information on social media, posted the stolen data on GitHub using their full name, and shared their hacking method with coworkers via Slack chat. An individual discovered the information on GitHub and alerted the financial company. The incident resulted in a cost of $150 million cost for the company.

## IT Security Analyst Launched Secondary Ransomware Attack

A former employee of a pharmaceutical drug development and manufacturing company plead guilty to using an existing ransomware attack to launch their own separate attack. The former IT security analyst was tasked with assisting the investigation into the initial ransomware incident, but instead launched a secondary ransomware attack.[[21]](#footnote-22) The employee set up an email address similar to the attacker’s email address and placed their own Bitcoin payment address in place of the attacker’s in emails to management. The employee also used the fake email address to pressure the company to pay the ransom. The ransom payment was never made as the employees’ access to private emails was discovered during the law enforcement investigation.[[22]](#footnote-23)

# Appendix D: Attacks and Threats

## Data Loss and Data Theft

Data theft and malicious data loss is a type of cybercrime where criminals gain access to sensitive and private information that is not meant to be shared publicly. This data can be as simple as names and addresses and escalate to social security numbers and banking information. Once the information has been ascertained the data is often copied and used to commit the crime of identity theft or as a way to exfiltrate money from victims. The economic and reputational impacts of data loss/theft on individuals and organizations can be significant. Losses can include: damage to productivity, continuity of operations disruption, financial cost from investigation and recovery, financial costs due to lawsuits from customers, employees, or regulatory penalties, and overall reputational damage. To mitigate data theft/loss it is necessary to know what personal and sensitive information is on your network or systems, know who has access to it, encrypt sensitive information, implement firewalls, apply network segmentation, and ensure your CIRP and Communications Plan include response and notification procedures for data breach incidents.

### Additional Resources

* CISA Continuous Diagnostics and Mitigation Program – Data Protection Management (<https://www.cisa.gov/sites/default/files/publications/2021-05-26_CDM%2520Data%2520Protection%2520Management%2520Fact%2520Sheet.pdf>)
* Protecting Sensitive and Personal Information (<https://www.cisa.gov/resources-tools/resources/protecting-sensitive-and-personal-information>)
* Cybersecurity and Physical Security Convergence Action Guide (<https://www.cisa.gov/resources-tools/resources/cybersecurity-and-physical-security-convergence-action-guide>)

## Insider Threat

An insider threat refers to the potential of an individual with authorized access or knowledge within an organization to cause harm. The threats posed by insiders include theft, espionage, violence, and sabotage involving technology, virtual reality, computers, devices, and the internet. Unintentional threats involve the non-malicious (accidental or inadvertent) exposure of an organization’s IT infrastructure, systems, and data leading to unintended harm. On the other hand, intentional threats involve malicious actions conducted by insiders with malicious intent, using technical means to disrupt business operations, identify IT weaknesses, access protected information, or advance an attack plan through IT system access. Such actions may include altering data, inserting malware, or deploying other offensive software to disrupt networks and systems. To successfully mitigate insider threats and implement effective insider threat programs, it is necessary to detect and identify observable, concerning behaviors or activities, followed by the subsequent implementation of measures aimed at managing the risk of potential harmful actions.

### Additional Resources

* CISA Insider Threat Mitigation Guide (<https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide>)
* Insider Threat Mitigation (<https://www.cisa.gov/topics/physical-security/insider-threat-mitigation>)

# Appendix E: Contacts and Resources

Federal Government Resources

* 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 Office Cyber Task Forces (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)

State Level Resources

* Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: [info@msisac.org](mailto:info@msisac.org); 518-266-3460)
* National Governors Association (NGA) (<https://www.nga.org/>)
  + NGA Center for Best Practices (<https://www.nga.org/bestpractices/divisions/hsps/>)
* DHS Cybersecurity Fusion Centers (<https://www.dhs.gov/state-and-major-urban-area-fusion-centers>)
* National Association of State Chief Information Officers (NASCIO) (<https://www.nascio.org/>)

Preparedness Resources

* CISA Cross-sector Cybersecurity Performance Goals (<https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist>)
* NIST Cybersecurity Framework Tools (<https://csf.tools/>)
* Insider Threat:
  + CISA Insider Threat Mitigation Guide (<https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide>)
  + CISA Insider Threat Mitigation (<https://www.cisa.gov/topics/physical-security/insider-threat-mitigation>)
  + NIST Insider Threat Program Management ([PM-12: Insider Threat Program - CSF Tools](https://csf.tools/reference/nist-sp-800-53/r5/pm/pm-12/))
* Ransomware:
  + 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>)

Additional Resources

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

1. “Computer Security Resource Center Glossary: Cyber Resilience,” National Institute of Science and Technology, accessed August 2, 2023, <https://csrc.nist.gov/glossary/term/cyber_resiliency>. [↑](#footnote-ref-2)
2. NIST CSF Tools, “Security Alerts, Advisories, and Directives,” <https://csf.tools/reference/nist-sp-800-53/r5/si/si-5/> [↑](#footnote-ref-3)
3. CISA CPG Checklist, “3.A Detecting Relevant Threats and TTPs,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-4)
4. CISA CPG Checklist, “2.L Secure Sensitive Data,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-5)
5. CISA Threat Mitigation Guide, “Detecting and Identifying Inisder Threat, “<https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide> [↑](#footnote-ref-6)
6. CISA CPG Checklist, “1.H Supply Chain Vulnerability Disclosure,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-7)
7. CISA CPG Checklist, “2.R System Backups,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-8)
8. CISA CPG Checklist, “2.T Log Collection,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-9)
9. NIST CSF Tools, “Account Management,” <https://csf.tools/reference/critical-security-controls/version-8/csc-5/> [↑](#footnote-ref-10)
10. CISA CPG Checklist, “2.F Network Segmentation,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-11)
11. NIST CSF Tools, “Asset vulnerabilities are identified and documented,” <https://csf.tools/reference/nist-cybersecurity-framework/v1-1/id/id-ra/id-ra-1/> [↑](#footnote-ref-12)
12. NIST CSF Tools, “Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value,” <https://csf.tools/reference/nist-cybersecurity-framework/v1-1/id/id-am/id-am-5/> [↑](#footnote-ref-13)
13. CISA CPG Checklist, ”2.S Incident Response (IR) Plans,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-14)
14. CISA CPG Checklist, “1.B Organizational Cybersecurity Leadership“ <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-15)
15. NIST CSF Tools, “Correlation with External Organizations,” <https://csf.tools/reference/nist-sp-800-53/r5/ir/ir-4/ir-4-8/> [↑](#footnote-ref-16)
16. NIST CSF Tools, “Business Contonuity Planning,” <https://csf.tools/reference/cloud-controls-matrix/version-3-0-1/bcr/bcr-01/> [↑](#footnote-ref-17)
17. CSF Tools, “Chain of Custody”, <https://csf.tools/reference/nist-sp-800-53/r5/au/au-10/au-10-3/> [↑](#footnote-ref-18)
18. S. Fadilpašić, “Cash App alerts 8 million customers to data breach,” *Tech Radar,* April 6, 2022, <https://www.techradar.com/news/cash-app-alerts-8-million-customers-to-data-breach>. [↑](#footnote-ref-19)
19. S. Wadhwani, “Block’s Cash App Suffers Serious Insider Theft, Customers’ Brokerage Accounts Compromised,” *Spiceworks,* April 6, 2022, <https://www.spiceworks.com/it-security/data-security/news/block-cash-app-data-insider-theft/>. [↑](#footnote-ref-20)
20. # Rob McLean, ” A hacker gained access to 100 million Capital One credit card applications and accounts,” *CNN,* July, 30 2019,

    <https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html>. [↑](#footnote-ref-21)
21. Gee Harland and Tom Seaward, “Letchworth man guilty of Oxford Biomedica ‘blackmail’” *Oxford Mail,* May 22, 2023, <https://www.oxfordmail.co.uk/news/23538315.ashley-liles-letchworth-man-guilty-oxford-biomedica-blackmail/>. [↑](#footnote-ref-22)
22. Pieter Arntz, “Employee guilty of joining ransomware attack on his own company,” Malwarebytes, May 23, 2023, <https://www.malwarebytes.com/blog/news/2023/05/employee-pleads-guilty-to-blackmail-and-unauthorized-access-after-5-years>. [↑](#footnote-ref-23)