

**CISA Tabletop Exercise Package Critical Manufacturing Sector**

[Enter Organization Name]

<Exercise Date>

Updated November 2023

Cybersecurity and Infrastructure Security Agency

Table of Contents

[Handling Instructions 3](#_Toc148992069)

[Exercise Overview 5](#_Toc148992075)

[General Information 6](#_Toc148992076)

[Module 1 8](#_Toc148992077)

[Module 2 11](#_Toc148992078)

[Appendix A: Additional Discussion Questions 13](#_Toc148992079)

[Appendix B: Acronyms 16](#_Toc148992080)

[Appendix C: Case Studies 17](#_Toc148992081)

[Appendix D: Malicious Activity 18](#_Toc148992082)

Appendix E: IT and OT Risk Mitigation ………………………………………………………………………………….19

[Appendix F: Contacts and Resources 21](#_Toc148992083)

# 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 <Critical Manufacturing Sector Organization> in response to a significant cyber incident. | |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Govern, Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Examine the response capabilities of <Critical Manufacturing Sector Organization> during a significant cyber incident. 2. Assess information sharing, notification, and coordination processes during a cyber incident. 3. Identify areas of improvement in cyber incident response plans and overall organizational resilience before, during, and following a significant cyber incident. | |
| Threat or Hazard | Cyber Incident | |
| Scenario | A malicious actor uses a phishing email as an entry point to networks/systems. Attackers compromise information technology (IT) and operational technology (OT) networks, resulting in a shutdown of operations. | |
| 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 (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 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)

## 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 attack types presented in this scenario.
* Appendix E: An overview of risk mitigation techniques for IT and OT systems.
* Appendix F: 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. Players may include IT/information security personnel, OT personnel, emergency management personnel, and representatives from legal/general counsel.

**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 staff such as management/leadership and personnel without a role in a cyber incident/emergency management.

**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 potential insider threat activity and the confirmation from a vendor that a suspicious email your employees received was not legitimate.
  + **Module 2:** This module continues the scenario with the discovery of propriety information/trade secrets found on the Dark Web, personnel locked out of the operating system for your Programmable Logic Controller (PLC) and concludes with a shutdown of operations.
* 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

CISA and the Federal Bureau of Investigation (FBI) release a joint cybersecurity advisory (CSA) to disseminate known tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) identified through FBI investigations of a sophisticated criminal group responsible for a string of attacks perpetrated against critical manufacturing organizations. The group demonstrates the capability to compromise IT networks; develop mechanisms to maintain long-term, persistent access to IT networks; exfiltrate sensitive data from IT and OT networks; and disrupt critical industrial control systems (ICS)/OT functions by deploying destructive malware.

Observed operations of the group include the deployment of destructive malware against critical manufacturing sector organizations.[[2]](#footnote-3) Attacks by this group against critical manufacturers were covered by national news media over the past year.

## 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 threat information is most useful?
   2. How is information disseminated to the relevant parties within your organization?
   3. What actions would your organization take in response to the report like the one presented in the scenario?
3. Discuss your organization’s cyber resilience planning.
   1. How are IT and OT business continuity functions coordinated?
   2. What IT and OT infrastructure has been identified to support mission essential functions in continuity of operations and incident response plans?
   3. How has cybersecurity been integrated into your continuity plans?

### Day 5

Members of the <Production Planning and Supply Chain Management> team at your organization request the addition of new software to the network. They say the software is a new tool that will help them enhance the efficiency of your organization’s operations and claim their manager expects this is done immediately.

1. Describe your organization’s asset management plan and how you prioritize critical assets.
   1. How does your organization maintain availability of key assets (e.g., network connectivity, etc.)?

### Day 7

Your organization uses legacy and proprietary operating systems to manage factory operations. The vendor for these operating systems arrives for an unscheduled visit to update IT and OT systems.

1. Describe the risks and advantages to maintaining legacy equipment/systems.
2. How do you manage technology that is no longer supported by the manufacturer?
3. What supply chain concerns do you have regarding legacy equipment/systems?
4. Describe your organization’s equipment commissioning and decommissioning process.
5. Describe your organization’s network configuration and your approach to network segmentation of IT and OT systems.
6. Describe your organization’s patch management and vulnerability management plans.
7. Does your organization apply Zero Trust Architecture (ZTA)/zero-trust concepts?
8. What level of access do your third-party vendors have to your organization’s network?[[3]](#footnote-4)
9. How often are third-party access rights and data logs reviewed?

### Day 9

Employees receive an email from one of your organization’s vendors advertising free tickets to an upcoming sporting event in the area. The email instructs employees to click on the link to claim these tickets.

1. Describe your organization’s cybersecurity training program for employees.[[4]](#footnote-5)
   1. How often are employees required to complete this training?
   2. Describe the cross-training or the coordination between the IT and OT departments.
   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?
2. What are your organization’s policies or procedures for IT account management?
   1. What are the protocols for establishing, activating, modifying, disabling, and removing accounts?
3. How do employees report suspected phishing attempts or other possible cybersecurity incidents?
   1. What actions does the IT department take when suspicious emails are reported?
   2. What feedback do employees receive after reporting a suspicious email or event?

### Day 15

The vendor who emailed your organization’s employees with the offer for free tickets discloses they were the target of a malware attack that compromised their business email.[[5]](#footnote-6) They confirm the email your employees received came from their system but was not sent by them. They also confirm that the site accessed through the link in the spoofed email was not legitimate.[[6]](#footnote-7)

1. What is the role of cybersecurity in the review and selection of third-party vendor support?[[7]](#footnote-8)
2. What cybersecurity language, (e.g., cybersecurity training and cyber incident notification requirements), is included within third-party vendor contracts?
3. How do you evaluate the cybersecurity posture of your vendors?
4. How often are contracts reviewed?

# Module 2

### Day 20

A freelance security researcher uncovers a series of posts on the Dark Web advertising the sale of <proprietary information/trade secrets> from your organization and reaches out to your Chief Information Security Officer (CISO). The posts advertise the sale of your organization’s information. Your insider risk team confirms the exfiltration of data noted by the security researcher.[[8]](#footnote-9)

## Discussion Questions

1. How would your organization respond to the theft and publishing of <proprietary information/trade secrets> on the Dark Web?
2. What role does your legal department play in cyber incident response?

### Day 22 - Morning

Several employees contact the help desk with complaints of difficulties accessing information on shared network drives. Some files were renamed, moved, or deleted. The IT department can recover the missing files from backups, but any work completed following the creation of the latest back-up has been lost.

1. Does your organization have backups of vital records stored in a location separate from your primary working files/copies?[[9]](#footnote-10)
2. How frequently do you restore from backups?
3. How long do you keep copies of archived files backed up?
4. How long would it take to restore primary files from backups? Have you tested restoration from backups?

### Day 22 – Afternoon

PLCs in your factory interact directly with the internet. These PLCs start malfunctioning, creating a disruption to your production processes. Personnel are unable to access the PLC operating system, PLC related data is encrypted, and employees from both the IT and OT departments are locked out of their user accounts.

1. What are the impacts to your organization’s operations if PLCs are not functional?
2. What redundant systems exist for when primary systems are compromised?
3. What alternative systems or manual processes do you implement to continue operations if a critical system is unavailable for a significant period?
4. Who can authorize use of alternate systems or procedures?
5. How long can you perform manual or alternate processes on your critical systems?
6. What resources do you have for additional staffing requirements?

### Day 29

It has been over a week and the operating system for the PLCs is still locked. Your organization is currently running backup manual operations.

The security researcher contacts your CISO again to report another post on the Dark Web regarding a cybercriminal using Known Exploited Vulnerabilities (KEVs) to compromise your PLC operating system.

1. What information are you sharing internally (e.g., employees, leadership)?[[10]](#footnote-11)
2. What information are you sharing externally (e.g., customers, vendors)?
3. How are third-party vendors involved in your incident response?
   1. How is this documented in your Cyber Incident Response Plan (CIRP)?
4. What legal and regulatory notifications are required based on the scenario?
   1. When are notifications made and who is responsible for making the notifications?
5. How sufficient are your organization’s current internal resources for responding to the cyber incidents in this scenario?
6. What additional resources outside of your organization are necessary for responding to the cyber incident?
7. What are the processes or procedures for requesting additional resources?
8. What external partners (e.g., CISA, FBI, etc.) would you contact for assistance?
9. 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 paragraph, as well as undesired discussion questions, should be deleted.*

## Cyber Resilience

1. Discuss how cyber preparedness is integrated with 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. Discuss your risk management strategy.
4. How is it developed/maintained?
5. What considerations are addressed in your risk management strategy (e.g., extended downtime, impaired functionality, loss of data, etc.)?
6. Describe your organization’s review process for your cyber incident response plan (CIRP).
7. How is your CIRP integrated with other incident or emergency response/management plans?
8. How often is the CIRP reviewed?
9. Which individual(s) and department(s) are responsible for reviewing and updating the plan?
10. How are updates to the plan communicated to department or agency employees?
11. Discuss your supply chain concerns related to your IT/OT infrastructure.
12. What is your method for tracking and identifying firmware vulnerabilities in your network?
13. 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?
14. How is the integrity of your critical data protected and validated?
15. What external entities have access to your data?
16. How would those entities report a compromise of their systems to your office?
17. What essential functions are impacted by the incidents described in the scenario?
18. If primary communications are compromised, how do you provide information to internal and external entities?
19. What policies and procedures does your organization use to decide when and how to restore backed-up data?
20. How does your organization incorporate measures for ensuring the integrity of backup data before restoration?

## 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 key, 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, 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 needs to 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 are your processes for collecting evidence and maintaining the chain of custody during a cyber incident?
2. At what point in the scenario would you contact law enforcement?
   1. How would a law enforcement investigation impact containment, eradication, and recovery efforts?
3. What are the processes for contacting critical personnel outside of core hours?
4. How do you proceed if critical personnel are unreachable or unavailable?
5. How would a breach of vendor(s) affect your organization if they have access to your information?
6. 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. Describe 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 exercises?
5. What external agencies are involved in the exercise?
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 a cybersecurity exercise?

## 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/Emergency Operations Center?
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. 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 documents does your organization have for cyber incidents?

# Appendix B: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| BYOD | Bring Your Own Device |
| CIRP | Cyber Incident Response Plan |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CISO | Chief Information Security Officer |
| CPG | Cybersecurity Performance Goals |
| CSF | Cybersecurity Function |
| CTEP | CISA Tabletop Exercise Package |
| FBI | Federal Bureau of Investigation |
| HR | Human Resources |
| ICS | Industrial Control System |
| IT | Information Technology |
| KEV | Known Exploited Vulnerabilities |
| NCEP | National Cyber Exercise Program |
| NIST | National Institute of Standards and Technology |
| OT | Operational Technology |
| PII | Personally Identifiable Information |
| PLC | Programmable Logic Controller |
| POC | Point of Contact |
| TLP | Traffic Light Protocol |
| ZTA | Zero Trust Architecture |

# Appendix C: Case Studies

## Ransomware Attack Against Agricultural Equipment Manufacturer

On May 5, 2022, the ransomware group Black Basta launched a ransomware attack against an agricultural equipment manufacturer. On May 16 the agricultural manufacturer announced data exfiltration occurred and the extent of the damage to their systems was still unknown, and that recovery may take longer than expected.[[11]](#footnote-12) Production halted at some company facilities until May 22. The delayed production schedules resulted in an increase in production for the remainder of 2022. The attackers also stole personally-identifiable information (PII) of company employees. The Black Basta group purchased user credentials on the dark web to infiltrate the company systems, and then relied on human error to errantly approve a run-as-administrator prompt.[[12]](#footnote-13)

## Ransomware Attack Against Tire and Materials Manufacturer

A ransomware attack struck a major tire and materials manufacturer on February 27, 2022, causing a halt in production capabilities for its North and Central American facilities. The LockBit ransomware group, responsible for the attack, also accessed sensitive data and production systems. The manufacturing company decided to take their facilities offline to prevent further damage and data exfiltration. The shut down lasted a week while the company ran a comprehensive security check on their systems.[[13]](#footnote-14) Six months later, on August 31, the manufacturer reported to the Attorney General of Massachusetts that the assailants obtained PII of their consumers. The PII included names, Social Security numbers, and banking information. This was part of LockBit’s string of cyberattacks, and the group threatened to release the information if their ransom demands were not met.[[14]](#footnote-15)

## Vulnerability in Industrial Controllers

CISA issued an advisory in February 2021 following the revelation that industrial controllers used around the country were vulnerable to unauthorized remote access and modification. A widely used series of industrial controllers used a secret key to verify communication between the Logix controllers and manufacturing machines they controlled. Minimally skilled hackers could remotely access the key and then use it to manipulate the controller, affecting production lines. The vulnerability could not be patched.[[15]](#footnote-16) CISA provided mitigation steps to those who used the products. For most models, companies had little choice but to lock down the controllers out of remote access capabilities, and some locked down the Internet entirely.[[16]](#footnote-17)

# Appendix D: Malicious Activity

## 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

* 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>)

## Social Engineering and Phishing

One of the most prominent tactics attackers use to exploit network and system vulnerabilities is social engineering, which is the manipulation of users through human interaction and the formation of trust and confidence to compromise proprietary information. Techniques for uncovering this information largely involve the use of phishing, i.e., email or malicious websites that solicit personal information by posing as a trustworthy source. Social engineering is effective for breaching networks and evading intrusion detection systems without leaving a log trail, and it is completely dependent on the operating system platform. While technical exploits aim to bypass security software, social engineering exploits are more difficult to guard against due to the involvement of human emotions. Organizations should take steps towards strengthening employee cybersecurity awareness training by incorporating trainings on identifying suspicious emails, instructing personnel on how to report them, and emphasizing the importance of keeping software systems up to date.

### 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>)

# Appendix E: IT and OT Risk Mitigation

## Boundary Protection

One of the most fundamental characteristics of a secure ICS network is the design and deployment of boundary protection. Boundary protection is the electronic division between ICS and enterprise networks. If boundary protection is not developed thoroughly, access to ICS networks can be manipulated via enterprise networks and other internet connected devices. Inadequate boundary protection can also make it difficult to detect unauthorized activity on ICS systems. To mitigate threats against network boundaries, limit the number of external networks to the system; implement a managed interface for each external telecommunication service; deny network communications traffic by default and allow network communications traffic by exception; detect and deny outgoing communications traffic posing a threat to external systems; and enforce adherence to protocol formats. For more information on boundary protection refer to the resource below.

*Additional Resources*

* NIST SP 800-53, Rev. 5.1.1.: “System and Communications Protection (SC) – Boundary Protection”(<https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=SC-07>)
* Layering Network Security Through Segmentation (<https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf>)

## Principle of Least Functionality

The principle of least functionality states that information systems should be configured to provide only essential capabilities and restrict or prohibit the use of non-essential functions, such as ports, protocols, and/or services that are not a key part of the industrial control system.[[17]](#footnote-18) Systems which are not structured using this principle have increased vectors for malicious parties to access. To implement the principle of least functionality, configure information systems to provide only essential capabilities; limit component functionality to a single function per device; disable any functions, port, protocol, and services that are deemed unnecessary; and identify and remove unauthorized/unsecure function, ports, protocol, services, and applications.

*Additional Resources*

* NIST SP 800-171, Rev. 3.0.0: “03.04: Configuration Management” (<https://csrc.nist.gov/pubs/sp/800/171/r3/final>)
* NIST Guide for Security Focused Configuration Management of Information Systems (<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf>)

## Physical Access Control

Physical access to assets should be managed and protected. Unauthorized physical access to field equipment provides a malicious actor the opportunity to modify, delete, or copy critical device programs and firmware. Malicious actors can also gain access to ICS networks and steal or vandalize cyber assets. Additionally, unprotected physical access locations present threat actors with an opportunity to add rouge devices to capture and retransmit network traffic. To mitigate threats against physical access control locations, develop, document, and disseminate a physical and environmental protection policy; maintain a list of individuals with authorized access to the facility where ICS systems reside; enforce physical access authorization; control physical access; monitor physical access; maintain visitor access logs; and protect equipment for the ICS system from damage and destruction.

*Additional Resources*

* NIST Cybersecurity Framework, v2.0 (via NIST CSRC CPRT), PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk. (<https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.AA-06>)
* Interagency Security Committee (ISC) Best practices for Facility Access Control (<https://www.cisa.gov/resources-tools/resources/isc-best-practices-facility-access-control>)
* Recommended Cybersecurity Practices for Industrial Control Systems (<https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf>)

# Appendix F: 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)

Critical Manufacturing Sector Resources

* CISA Critical Manufacturing Sector Resources (<https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/critical-manufacturing-sector>)
* CISA Cyber Threats to Critical Manufacturing Sector ICS (<https://www.cisa.gov/sites/default/files/publications/CISA%20Insight%20Control%20Systems%2023Dec2021_508%20Updated.pdf>)
* CISA/Department of Energy Recommended Cybersecurity Practices for ICS (<https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf>)
* NIST Special Publication 800-82r3 Guide to OT Security (<https://www.nist.gov/news-events/news/2023/09/nist-publishes-guide-operational-technology-ot-security>)

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 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/>)

Private Sector/Business 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/))

Preparedness Resources

* 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))

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. CISA, “Alerts and Advisories,” <https://www.cisa.gov/news-events/cybersecurity-advisories>. [↑](#footnote-ref-3)
3. NIST Cybersecurity Framework, v2.0 (CSF 2.0) via NIST’s CPRT, “PR.AA: Identity Management, Authentication, and Access Control,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.AA>. [↑](#footnote-ref-4)
4. NIST CSF 2.0 via CPRT, “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-5)
5. NIST CSF 2.0 via CPRT, “GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=GV.SC-05>. [↑](#footnote-ref-6)
6. NIST CSF 2.0 via CPRT, “ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.IM-04>. [↑](#footnote-ref-7)
7. NIST CSF 2.0 via CPRT, “GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=GV.SC-08>. [↑](#footnote-ref-8)
8. NIST CSF 2.0 via CPRT, “RS.CO-03: Information is shared with designated internal and external stakeholders,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RS.CO-03>. [↑](#footnote-ref-9)
9. NIST CSF 2.0 via CPRT, “PR.DS-11: Backups of data are created, protected, maintained, and tested,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.DS-11>. [↑](#footnote-ref-10)
10. NIST CSF 2.0 via CPRT, “GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=GV.RR-02>. [↑](#footnote-ref-11)
11. Greg Peterson, “AGCO Provides Update on Recovery from Ransomware Cyber Attack,” *AGCO*, May 16, 2022, [Ahttps://news.agcocorp.com/2022-05-16-AGCO-Provides-Update-on-Recovery-from-Ransomware-Cyber-Attack](https://news.agcocorp.com/2022-05-16-AGCO-Provides-Update-on-Recovery-from-Ransomware-Cyber-Attack). [↑](#footnote-ref-12)
12. Mihir Bagwe, “Black Basta Claims Responsibility for AGCO Attack,” *Bankinfo Security*, May 26, 2022, [https://www.bankinfosecurity.com/black-basta-claims-responsibility-for-agco-attack-a-19146](https://urldefense.us/v3/__https:/www.bankinfosecurity.com/black-basta-claims-responsibility-for-agco-attack-a-19146__;!!BClRuOV5cvtbuNI!G5S3nWzpx3Hh1pizLQDR9BFZasiEBSDK2PVGfuGkZdw7txTAbbZ3kzYFO_KnO6H5ofQ-WZT9hs8-zWgbpAfwMUBZzkNatynSFDI$). [↑](#footnote-ref-13)
13. Mariko Katsumara, “Japan's Bridgestone reports ransomware attack at U.S. subsidiary,” *Reuters*, March 18, 2022, [https://www.reuters.com/business/autos-transportation/japans-bridgestone-reports-ransomware-attack-us-subsidiary-2022-03-18/](https://urldefense.us/v3/__https:/www.reuters.com/business/autos-transportation/japans-bridgestone-reports-ransomware-attack-us-subsidiary-2022-03-18/__;!!BClRuOV5cvtbuNI!G5S3nWzpx3Hh1pizLQDR9BFZasiEBSDK2PVGfuGkZdw7txTAbbZ3kzYFO_KnO6H5ofQ-WZT9hs8-zWgbpAfwMUBZzkNaNwPztC8$). [↑](#footnote-ref-14)
14. Richard Console Jr., “Bridgestone Americas, Inc. Releases Additional Details About February 2022 Ransomware Attack,” *JDSupra*, September 1, 2022, [https://www.jdsupra.com/legalnews/bridgestone-americas-inc-releases-6242225/](https://urldefense.us/v3/__https:/www.jdsupra.com/legalnews/bridgestone-americas-inc-releases-6242225/__;!!BClRuOV5cvtbuNI!G5S3nWzpx3Hh1pizLQDR9BFZasiEBSDK2PVGfuGkZdw7txTAbbZ3kzYFO_KnO6H5ofQ-WZT9hs8-zWgbpAfwMUBZzkNaiMVS_JQ$). [↑](#footnote-ref-15)
15. Dan Goodin, “Hard-coded key vulnerability in Logix PLCs has severity score of 10 out of 10,” *Ars Technica*, February 26, 2021, [https://arstechnica.com/information-technology/2021/02/hard-coded-key-vulnerability-in-logix-plcs-has-severity-score-of-10-out-of-10/#:~:text=The%20vulnerability%2C%20which%20is%20tracked,communication%20between%20the%20two%20devices](https://urldefense.us/v3/__https:/arstechnica.com/information-technology/2021/02/hard-coded-key-vulnerability-in-logix-plcs-has-severity-score-of-10-out-of-10/*:*:text=The*20vulnerability*2C*20which*20is*20tracked,communication*20between*20the*20two*20devices__;I34lJSUlJSUlJSU!!BClRuOV5cvtbuNI!G5S3nWzpx3Hh1pizLQDR9BFZasiEBSDK2PVGfuGkZdw7txTAbbZ3kzYFO_KnO6H5ofQ-WZT9hs8-zWgbpAfwMUBZzkNaQRjCjDU$). [↑](#footnote-ref-16)
16. “Rockwell Automation Logix Controllers (Update A),” *Cybersecurity & Infrastructure Security Agency*, March 18, 2021, <https://www.cisa.gov/news-events/ics-advisories/icsa-21-056-03>. [↑](#footnote-ref-17)
17. Georgetown University Information Security Office, “Least Functionality Guidelines,” “[UIS.203.7 Leahttps://security.georgetown.edu/config-mgt-policy/least-functionality-guidelines/#:~:text=The%20principle%20of%20least%20functionality%20provides%20that%20information,integral%20to%20the%20operation%20of%20that%20information%20system.st Functionality Guidelines | University Information Security Office | Georgetown University](https://security.georgetown.edu/config-mgt-policy/least-functionality-guidelines/#:~:text=The%20principle%20of%20least%20functionality%20provides%20that%20information,integral%20to%20the%20operation%20of%20that%20information%20system.)”. [↑](#footnote-ref-18)