# 

**CISA Tabletop Exercise Package Industrial Control Systems**

# [Enter Organization Name]

# <Exercise Date>

Updated July 2024

Cybersecurity and Infrastructure Security Agency

Table of Contents

[Handling Instructions 3](#_Toc169776626)

[General Information 5](#_Toc169776632)

[Exercise Overview 8](#_Toc169776633)

[Module 1 9](#_Toc169776634)

[Module 2 11](#_Toc169776635)

[Appendix A: Additional Discussion Questions 13](#_Toc169776636)

[Appendix B: Case Studies 17](#_Toc169776637)

[Appendix C: Malicious Activity 18](#_Toc169776638)

[Appendix D: IT and OT Risk Mitigation 19](#_Toc169776639)

[Appendix E: Contacts and Resources 21](#_Toc169776640)

[Appendix F: Acronyms 22](#_Toc169776641)

# 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 (TTX). A TTX 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. 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). 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: An overview of risk mitigation techniques for Information Technology (IT) and Operational Technology (OT) systems.
* Appendix F: 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, OT personnel, emergency management personnel, security personnel, human resources personnel, legal personnel, 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, OT personnel, emergency management personnel, security personnel, legal personnel, 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 modernization of technology to the cloud, a possible phishing attempt, and odd vendor activity.
  + **Module 2:** This module includes reports of service disruptions, industrial control systems (ICS) failures, and malware.
* 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.[[2]](#footnote-3)

# 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 | Assess the cyber resilience of <Organization> and their ability to secure their industrial control systems (ICS) against cyber threats. | |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Govern, Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Assess the resilience of <Organization> during and following a cyber incident impacting ICS. 2. Improve IT and OT cybersecurity coordination to enhance organizational cybersecurity posture. 3. Evaluate the ability to restore operations after disruptions from cyber intrusions. | |
| Threat or Hazard | Cyber Incident | |
| Scenario | During a transition of systems to the cloud, employees receive a possibly fraudulent email, encounter odd vendor activity, and detect suspicious network traffic. After receiving reports of service disruptions, ICS failures occur, and malware encrypts systems. | |
| 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) | | |

# Module 1

### Day 1

The Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) release a joint alert regarding a cyber campaign targeting organizations in your sector over the past several months.[[3]](#footnote-4) Malicious actors are using sophisticated phishing schemes combined with social engineering tactics to circumvent multi-factor authentication (MFA) security measures. These malicious actors seek to compromise ICS with the intent to disrupt operations and extort victims.

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. Discuss your organization’s cyber resilience planning.
   1. How are IT and OT business continuity functions coordinated?
   2. What IT and OT infrastructure supports your essential functions, as documented in continuity of operations and incident response plans?
   3. Does your organization apply Zero Trust Architecture (ZTA)/zero-trust concepts?[[4]](#footnote-5)
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 an alert like the one presented in the scenario?

### Day 4

Your organization’s IT and OT teams are working on a technology modernization project at your facility. This project involves multiple IT/OT vendors to assist with the development of cloud infrastructure to support ICS. This project also involves implementation of a remote access solution for technicians to monitor and control OT systems.

1. Describe your organization’s asset management plan and how you prioritize critical assets.
   1. How does your organization maintain availability of critical or key assets (e.g., network connectivity)?
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. Describe the risks/advantages to maintaining legacy equipment/systems.
   1. How do you manage technology that is no longer supported by the manufacturer?
   2. What supply chain concerns do you have regarding legacy equipment/systems?
   3. Describe your organization’s equipment commissioning and decommissioning processes.
4. What level of access do your third-party vendors have to your organization’s network?
   1. How often are third-party access rights and data logs reviewed?
   2. What mechanisms or processes are in place to prevent malicious activity originating from vendors?

### Day 7

Several employees in the IT and OT departments receive an email that appears to be from the CEO.[[5]](#footnote-6) The email asks these employees to log in to a website to complete a questionnaire related to the ongoing modernization project. Some employees report the email as suspicious while others follow the link for the questionnaire.[[6]](#footnote-7)

### Day 8

Several employees receive repeated notifications from the MFA app on their phones to approve attempted log-ons. Some employees approve the requests.

1. Describe your organization’s cybersecurity training program for employees.
   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. 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?
   3. Does your organization employ phishing tests? If so, describe the conduct of the tests and how employees receive feedback/training following the tests.

### Day 15

An OT vendor is scheduled to install equipment at one of your organization’s remote facilities. A technician from your OT department calls from the remote facility to report the vendor did not show up at the scheduled time, but it appears that the equipment was already installed.

ICS monitoring tools do not report anything outside the baseline for your network.

1. What policies and procedures does your organization have to maintain the security of facilities, networks, and systems?
   1. What are your access control measures for both OT and IT assets and associated facilities?
   2. Where are these policies and procedures documented?

# Module 2

### Day 23

Your organization’s customer support center receives an influx of calls reporting service disruptions.

Later that day, technicians monitoring your organization’s various IT/OT systems notice lagging and distorted data inputs that impact their ability to monitor the equipment and processes.

## Discussion Questions

1. Discuss your organization’s intrusion detection capabilities and analytics that alert you to a potential cyber incident.
   1. What type of hardware and/or software does your organization use to detect and prevent malicious activity on your systems/network?
   2. How does your organization differentiate between various types of external scanning?

### Day 24

A system alarm alerts facility operators of <system failure of choice>, causing a shutdown of operations due to automatic emergency fail safes. Technicians cannot access ICS controls, <control logic, historian> data is encrypted, and several employees from your IT and OT departments report being locked out of their user accounts. During physical inspection of the failed components, technicians discover there is no physical reason for the failure.

1. Using your organization’s cyber incident response plan (CIRP), describe the actions your organization would take to minimize impact on current operations.
2. What guidance does the plan include on assessing the severity of the incident?
3. How does incident severity level dictate response?
4. How are critical systems and processes incorporated within your CIRP?
5. How does your CIRP/IT response plan incorporate OT incident response?
   1. Is your CIRP aligned with any OT incident response plans?
6. What redundant systems exist when primary systems are compromised?
7. What alternative systems or manual processes are implemented to continue operations if a critical system is unavailable for a significant period?
8. Does your CIRP include procedures to operate in manual mode if a cyber incident compromises OT systems?
9. Who authorizes the use of alternate systems or procedures?
10. How long can you perform manual or alternate processes?
11. Does your organization have backups of control files and other important files stored in a location separate from your primary working files/copies?[[7]](#footnote-8),[[8]](#footnote-9)
    1. How long would it take to restore primary files from backups?
    2. How frequently do you test restoration from backups?
    3. How long do you keep copies of archived files backed up?
12. What are the roles of your security operations center during a response?
13. Who is responsible for coordinating information across different organizational-level incidents?

### Day 25

Computers throughout your organization display a red screen with a message taking credit for the malfunctioning industrial processes and threatens to continue the IT/OT system lockout.

### Day 26

Security researchers disclose details of a critical vulnerability in the remote access solution shared on a hacker email list. Their report also includes information found on the dark web about Known Exploited Vulnerabilities used to compromise your organization’s various IT and OT components along with sensitive information offered for sale to the highest bidder.[[9]](#footnote-10)

1. How sufficient are your organization’s current internal resources for responding to the cyber incidents in this scenario?
2. What additional resources outside of your organization would be necessary for responding to the cyber incident?
3. What are the processes or procedures for requesting additional resources?
4. What external partners (e.g., CISA, FBI, etc.) would you contact for assistance?
5. What legal and regulatory notifications are required based on the scenario?
   1. When are notifications made and who is responsible for making the notifications?
6. 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 in the final version of the Situation Manual.*

## 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. Discuss your risk management strategy.
   1. How is it developed/maintained?
4. Describe your organization’s review process for your CIRP.
   1. How is your CIRP integrated with other incident or emergency response/management plans?
   2. How often is the CIRP reviewed?
   3. Which individual(s) and department(s) are responsible for reviewing and updating the plan?
   4. How are updates to the plan communicated to department or agency employees?
5. Discuss your supply chain concerns related to your IT/OT infrastructure.
6. What cybersecurity language is included within third-party vendor contracts?
7. How do you evaluate the cybersecurity posture of your vendors?
8. How often are contracts reviewed?
9. How do your service level agreements address cyber incident notification?
10. What level of access do your third-party vendors have to your organization’s network?
11. What mechanisms or processes are in place to prevent malicious activity?
12. Describe your organization’s approach to provisioning, revising, and removing vendor access to your organization’s network.
13. What is your method for tracking and identifying firmware vulnerabilities in your network?
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 your data?
17. How would those entities report a compromise of their systems to your office?
18. What essential functions are impacted by the incidents described in the scenario?
19. If primary communications are compromised, how do you provide information to internal and external entities?
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?
    2. How does your organization test your data backup plan?
21. Does your organization’s IT security team use any e-discovery/open source intelligence (OSINT) activities to identify internet facing vulnerabilities?

## Accounts & Privileges

1. Describe your organization’s employee off-boarding process.
2. Is this process coordinated with Information Technology (IT) and Human Resources (HR)?
3. Is this process coordinated with Operational Technology (OT)?
4. What additional actions are taken if the employee’s termination is contentious?
5. How 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 process?
6. Describe your organization’s bring your own device (BYOD) policy.
7. What are your organization’s policies or procedures for IT account management?
8. What are the protocols for establishing, activating, modifying, disabling, and removing accounts?
9. How do you confirm disabled/removed accounts are no longer active?

## 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 CIRP?
4. What cybersecurity incident escalation criteria is 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 would leadership be notified?
8. How often is your organization’s data reviewed?
9. 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. Are IT/OT system owners’ contact information documented in your response plans to ensure the correct personnel can be reached during a cyber event?
4. What are the processes for contacting critical personnel outside of core hours?
5. How do you proceed if critical personnel are unreachable or unavailable?
6. How would an incident at vendor(s) affect your organization if they have access to your information?
7. What are the notification requirements to your organization for incidents?

## 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?
   1. What additional training and/or exercise requirements do you require for your incident response staff?
2. How often does your organization exercise its CIRP?
3. Who is involved in the exercise?
4. How do your organization’s training and exercise efforts address both physical and cyber risks?
5. 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?
   1. How do these goals align with organizational objectives?
2. What cybersecurity training is required for senior leadership?
3. At what point would you activate your organization’s Security Operations Center/Emergency Operations Center?
4. What is your role during a cyber incident?
5. What information do you need to support your decision-making process?
6. What are the gaps in your cybersecurity workforce?
7. How does your organization recruit, develop, and retain cybersecurity staff?

## Public Information

* + - 1. Describe your organizational processes to respond to media reports and inquiries.
         1. How would you preserve and reinforce the public’s confidence and trust in your organization during a significant incident?
      2. What training is provided to employees regarding reporting contact with the media?
      3. How do you build and maintain trust with the public?

## Legal

1. What is the role of the legal counsel during a cyber incident?
2. What internal organizational legal guidance documents does your organization have for clients to use in planning for cyber incidents?
3. What are some examples of documents that you might request your legal counsel to help draft or provide legal review for in response to a cyber incident?

# Appendix B: 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.[[10]](#footnote-11) Production halted at some company facilities until May 22. The delayed production schedules resulted in an increased production pace for the remainder of 2022 in order to make up for the downtime during incident response and recovery. 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.[[11]](#footnote-12)

## 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.[[12]](#footnote-13) 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.[[13]](#footnote-14)

## 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.[[14]](#footnote-15) 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.[[15]](#footnote-16)

# 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 proprietary information. Common social engineering techniques involve 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 Multi-Factor Authentication (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>)

# Appendix D: IT and OT Risk Mitigation

## Boundary Protection

One of the most fundamental characteristics of a secure Industrial Control System (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 resources 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.[[16]](#footnote-17) 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; identify and remove unauthorized/unsecure functions, ports, protocols, services, and applications, and disable any that are authorized but not necessary.

*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 rogue 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 ICS system equipment 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 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://www.nist.gov/cyberframework>)
* ICS/OT:
  + 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>)
* Supply Chain:
  + CISA Supply Chain Resource Library (<https://www.cisa.gov/ict-supply-chain-resource-library>)
  + NIST Cybersecurity Supply Chain Risk Management (<https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/publications>)

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/))

# Appendix F: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| BYOD | Bring Your Own Device |
| CIRP | Cyber Incident Response Plan |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CPG | Cybersecurity Performance Goals |
| DDoS | Distributed Denial of Service |
| DHS | U.S. Department of Homeland Security |
| FBI | Federal Bureau of Investigation |
| HR | Human Resources |
| ICS | Industrial Control Systems |
| IT | Information Technology |
| NIST | National Institute of Standards and Technology |
| OSINT | Open Source Intelligence |
| OT | Operational Technology |
| PII | Personally Identifiable Information |
| TLP | Traffic Light Protocol |
| ZTA | Zero Trust Architecture |

1. “Computer Security Resource Center (CSRC) 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. FEMA, “Homeland Security Exercise and Evaluation Program,” January 2020, <https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep>. [↑](#footnote-ref-3)
3. CISA “Cybersecurity Alerts and Advisories,” <https://www.cisa.gov/news-events/cybersecurity-advisories>. [↑](#footnote-ref-4)
4. CISA Resources, “Zero Trust Maturity Model,” <https://www.cisa.gov/zero-trust-maturity-model>. [↑](#footnote-ref-5)
5. CSF 2.0 via CPRT, “PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.DS-02>. [↑](#footnote-ref-6)
6. 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-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, ”Protect: System Backups (2.R),” <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>. [↑](#footnote-ref-9)
9. CISA – Known Exploited Vulnerabilities (KEV) Catalog, <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>. [↑](#footnote-ref-10)
10. Greg Peterson, “AGCO Provides Update on Recovery from Ransomware Cyber Attack,” *AGCO*, May 16, 2022, [https://news.agcocorp.com/news/agco-provides-update-on-recovery-from-ransomware-cyber-attack](https://urldefense.us/v3/__https:/news.agcocorp.com/news/agco-provides-update-on-recovery-from-ransomware-cyber-attack__;!!BClRuOV5cvtbuNI!G5S3nWzpx3Hh1pizLQDR9BFZasiEBSDK2PVGfuGkZdw7txTAbbZ3kzYFO_KnO6H5ofQ-WZT9hs8-zWgbpAfwMUBZzkNaovZwYKw$). [↑](#footnote-ref-11)
11. Mihir Bagwe, “Black Basta Claims Responsibility for AGCO Attack,” *Bankinfo Security*, May 26, 2022, [https://www.bankinfosecurity.com/black-basta-claims-responsibility-for-agco-attack-a-19146](https://urldefense.us/v3/__https:/www.bankinfosecurity.com/black-basta-claims-responsibility-for-agco-attack-a-19146__;!!BClRuOV5cvtbuNI!G5S3nWzpx3Hh1pizLQDR9BFZasiEBSDK2PVGfuGkZdw7txTAbbZ3kzYFO_KnO6H5ofQ-WZT9hs8-zWgbpAfwMUBZzkNatynSFDI$). [↑](#footnote-ref-12)
12. 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$). [↑](#footnote-ref-13)
13. Richard Console Jr., “Bridgestone Americas, Inc. Releases Additional Details About February 2022 Ransomware Attack,” *JDSupra*, September 1, 2022, [https://www.jdsupra.com/legalnews/bridgestone-americas-inc-releases-6242225/](https://urldefense.us/v3/__https:/www.jdsupra.com/legalnews/bridgestone-americas-inc-releases-6242225/__;!!BClRuOV5cvtbuNI!G5S3nWzpx3Hh1pizLQDR9BFZasiEBSDK2PVGfuGkZdw7txTAbbZ3kzYFO_KnO6H5ofQ-WZT9hs8-zWgbpAfwMUBZzkNaiMVS_JQ$). [↑](#footnote-ref-14)
14. 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-15)
15. “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-16)
16. Georgetown University Information Security Office, “Least Functionality Guidelines,” <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.st Functionality Guidelines | University Information Security Office | Georgetown University>”. [↑](#footnote-ref-17)