

**CISA Tabletop Exercise Package Food and Agriculture Sector – Food Processing/Manufacturing Facilities**

[Enter Organization Name]

<Exercise Date>

Updated May 2024

Cybersecurity and Infrastructure Security Agency

Table of Contents

[Handling Instructions 3](#_Toc158021094)

[Exercise Overview 5](#_Toc158021100)

[General Information 6](#_Toc158021101)

[Module 1 8](#_Toc158021102)

[Module 2 10](#_Toc158021103)

[Appendix A: Additional Discussion Questions 12](#_Toc158021104)

[Appendix B: Acronyms 15](#_Toc158021105)

[Appendix C: Case Studies 16](#_Toc158021106)

[Appendix D: Malicious Activity 17](#_Toc158021107)

[Appendix E: IT and OT Risk Mitigation 19](#_Toc158021108)

[Appendix F: Contacts and Resources 21](#_Toc158021109)

# Handling Instructions

**Delete instructions that are not applicable.**

TLP:CLEAR

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

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

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

TLP:GREEN

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

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

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

TLP:AMBER

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

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

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

TLP:AMBER+STRICT

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

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

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

TLP:RED

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

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

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

# 

# Exercise Overview

|  |  |  |
| --- | --- | --- |
| Exercise Name | Exercise Name | |
| Exercise Date, Time, and Location | Exercise Date  Time (e.g., 9:00 a.m. – 12:00 p.m.)  Exercise Location | |
| Exercise Activities | Time | Activity |
| 20 Minutes | Threat Briefing and Opening Remarks |
| 60 Minutes | Module 1 |
| 20 Minutes | Break |
| 60 Minutes | Module 2 |
| 20 Minutes | Hotwash |
| Purpose | Examine the cyber resilience of <organization> in response to a cyber incident affecting the Food and Agriculture Sector. | |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Govern, Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Assess the cyber resilience of <organization> before, during, and following a cyber incident. 2. Examine plans, policies, and procedures in response to a cyber incident. 3. Assess information sharing, notification, and coordination processes with partners during a 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) 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. The footnotes in the modules contain corresponding resources intended to guide your preparedness efforts. The appendices provide the following information to tailor the exercise discussion:

* Appendix A: Additional discussion questions that can replace or augment the existing Module 1 and 2 discussion questions.
* Appendix B: Reference section for acronyms used within this situation manual.
* Appendix C: Case studies that provide real-world examples of the threats presented in this scenario.
* Appendix D: An explanation of the threats presented in this scenario.
* Appendix E: An overview of risk mitigation techniques for IT and Operational Technology (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, physical security and emergency management personnel, human resources and 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, physical security/emergency management personnel, human resources and 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 suspicious hyperlink in a newsletter received by employees, and an automatic alert from your Human Machine Interface (HMI) dashboard.
  + **Module 2:** This module continues the scenario with personnel locked out of your IT systems that leads to a shutdown of operations.
* Hotwash
* ***Structure Note:*** *Modules, timeline dates, and discussion questions included in each module may be modified as desired. Appendix A contains additional discussion questions for each module.*

## 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. The hotwash is held at the end of the exercise discussion. The hotwash is designed to provide an opportunity to discuss strengths and areas for improvement immediately following the conduct of an exercise.[[2]](#footnote-3)

# Module 1

### Day 1

Over the past year, multiple food and beverage processors and manufacturers were the target of ransomware attacks. These attacks resulted in the shutdown of production, leading to significant losses for the impacted organizations. The attacks received widespread media coverage, leading to a loss of public confidence in the safety of food and beverage products.

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) issued a joint cybersecurity advisory detailing the Tactics, Techniques, and Procedures (TTPs) used in the attacks over the past year, including gaining access to networks via phishing emails, theft of Remote Desktop Protocols (RDP) credentials, brute force attacks, and the exploitation of software vulnerabilities.[[3]](#footnote-4) The advisory urges organizations to update their operating systems and software, implement user training and phishing exercises, secure RDP, ensure there are offline backups of all critical data, and employ multifactor authentication.

## 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 advisory like the one presented in the scenario?
3. Discuss your organization’s cyber resilience planning.
4. What risk assessments have you conducted to identify specific cyber threats, vulnerabilities, and critical assets?[[4]](#footnote-5)
5. What improvements have you implemented to enhance cyber resilience following recent risk assessments?
6. Does your organization apply Zero Trust Architecture (ZTA)/zero-trust concepts?[[5]](#footnote-6)

### Day 6

Your organization begins the process of replacing legacy equipment with cloud-based HMI OT food/beverage processing tools to increase facility efficiency by better integrating OT systems with existing IT cloud-based systems.

1. Has your organization conducted a risk assessment to identify specific cyber threats, vulnerabilities, and critical assets?
   1. What IT and OT systems or processes are the most critical to your organization?
   2. Does your organization have a vulnerability management program dedicated to mitigating known exploited vulnerabilities in internet-facing systems?
2. Describe the risks and 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 or the procurement of new systems?
   3. Describe your organization’s equipment security commissioning and decommissioning processes.
3. Describe your organization’s asset management plan and how you prioritize critical assets.
4. Describe your organization’s patch management and vulnerability management plans.
   1. What processes are used to evaluate and maintain an allowed list of patches?
   2. How does risk inform decisions regarding allowed hardware, firmware, and software?
   3. What considerations (e.g., extended downtime, loss of data, impaired functionality, etc.) are addressed in the plan’s risk management strategy?

### Day 10

Several employees receive a monthly newsletter from a popular industry trade group that includes multiple embedded links.[[6]](#footnote-7) Some employees click on a link to enter to win a free trip to the industry conference sponsored by the trade group, where they are prompted to enter personal information.

1. Describe your organization’s cybersecurity training program for employees.[[7]](#footnote-8)
   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 users with system administrator-level privileges?
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?

### Day 23

The newly installed cloud-based HMI dashboard stops reporting data from <Programmable Logic Controllers or Remote Terminal Units> triggering an automatic alert. Physical inspection shows that the <systems/machinery> is operating normally.

1. How does your organization baseline network activity?[[8]](#footnote-9)
   1. How do you distinguish between normal and abnormal traffic?
   2. What are your next steps when abnormal activity is detected/reported?
   3. What indicators of compromise feeds does your organization use?

# Module 2

### Day 27: Morning

Computers on the <processing/facility> floor become unresponsive and operators are unable to regain control of the <manufacturing/processing> systems. They are forced to begin emergency shut down procedures for all operations. Office computers display a blank screen containing a ransom message demanding <insert ransom amount (e.g., $200,000.00)> worth of cryptocurrency for the decryption key and a warning that the key will expire unless payment is received within 48 hours.

## Discussion Questions

1. Explain your organization’s decision-making process regarding ransomware payment.
   1. Explain how your response partners, such as your cyber insurance provider or third-party vendors, are involved in your procedures.
   2. Discuss potential legal and reputational ramifications of paying or not paying the ransom.
2. What is the organizational policy for voluntarily reporting incidents to CISA or reporting to other government partners?
3. Using your organization’s cyber incident response plan (CIRP), describe the actions your organization would take to minimize impact on current operations.[[9]](#footnote-10)
   1. How does your plan define escalation criteria, notifications, activations, and/or courses of action?
   2. What guidance does the plan include for assessing the severity of the incident?
4. How does your CIRP/IT response plan incorporate OT incident response?
   1. Is your CIRP aligned with any OT incident response plans?

### Day 27: Afternoon

An internal investigation reveals that <proprietary information, intellectual property, and/or program control files> was/were copied and exfiltrated.

1. What policies and procedures does your organization use to decide when and how to restore backed-up data?[[10]](#footnote-11),
   1. How does your organization incorporate measures for ensuring the integrity of backup data before restoration?
2. What are the potential impacts of data theft to you organization?
   1. How does the type of stolen information (e.g., intellectual property vs. program control files) change the potential impacts?
   2. What redundant systems exist for when primary systems are compromised?
   3. How long can you perform manual or alternate processes on your critical systems?

### Day 28

Business partners and customers call your organization to request information about the expected timeline for system restorations. Many customers/partners also express concerns about widespread supply chain impacts if your operational delays continue.

1. What information are you sharing externally (e.g., customers, vendors) and internally (e.g., employees, leadership)?
   1. What sector partners do you collaborate with before, during, and after a cybersecurity incident?
   2. What actions can your organization take to mitigate reputational impacts because of these incidents?
2. What legal and regulatory notifications are required based on the scenario?
   1. When would notifications be made and who is responsible for making the notifications?

### Day 30

Investigation confirms the attacker entered systems via a malicious link in the trade newsletter your employee(s) clicked. Attackers moved laterally, gaining access across your IT systems, including access to your cloud-based HMI. Investigators also confirm the malicious actors posted part of your stolen data on the Dark Web and are attempting to sell the remainder of the data.

1. How does your organization determine when a cyber incident is over?
   1. Who makes this decision?
2. Based on the discussion, what changes will you implement to increase the resilience of your organization against future attacks?[[11]](#footnote-12)
   1. Describe the lessons learned and corrective action processes you use.
   2. What measures will you take to better secure your network?

# 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 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. Does your organization maintain a risk register that is consistently reviewed and discussed at an executive level?
7. Describe your organization’s review process for your CIRP.
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 cybersecurity language is included within third-party vendor contracts?
13. How do you evaluate the cybersecurity posture of your vendors?
14. How often are contracts reviewed?
15. How do your service level agreements address cyber incident notification?
16. What is your method for tracking and identifying firmware vulnerabilities in your network?
17. How is the integrity of your critical data protected and validated?
18. What external entities have access to your data?
19. How would those entities report a compromise of their systems to your organization?
20. What essential functions are impacted by the incidents described in the scenario?
21. If primary communications are compromised, how do you provide information to internal and external entities?

## 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 employee off-boarding process.
4. Is this process coordinated with IT and Human Resources (HR)?
5. What additional actions are taken if the employee’s termination is contentious?
6. 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)?

## Incident Identification

1. How are cyber incidents reported within your organization?
2. What would trigger the reporting requirements established by regulation, state law, and/or organization policy?
3. What training do employees receive regarding reporting requirements and your cyber incident response plan?
4. What cybersecurity incident escalation criteria is defined in your cyber incident response plan?
5. Who is responsible and what actions would they take based on the scenario?
6. Who 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. 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 involving your vendor(s) affect your organization if they have access to your information?

## Recovery

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

## Training & Exercises

1. What training does your cybersecurity incident response team undergo to detect, analyze, and report malicious activity?
2. What additional training and/or exercise requirements do you require for your incident response staff?
3. How often does your organization exercise its CIRP?
4. Who is involved in the exercises?
5. What external agencies are involved in the 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. 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. Who is responsible/authorized to speak to the media?
2. What training do employees receive on reporting contact with the media?

## 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 |
| AI | Artificial Intelligence |
| CIRP | Cyber Incident Response Plan |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CPG | Cybersecurity Performance Goals |
| CSF | Cybersecurity Function |
| CTEP | CISA Tabletop Exercise Package |
| FBI | Federal Bureau of Investigation |
| HMI | Human Machine Interface |
| HR | Human Resources |
| ICS | Industrial Control System |
| IT | Information Technology |
| NCEP | National Cyber Exercise Program |
| NIST | National Institute of Standards and Technology |
| OT | Operational Technology |
| RDP | Remote Desktop Protocol |
| TLP | Traffic Light Protocol |
| TTP | Tactics, Techniques, and Procedures |
| ZTA | Zero Trust Architecture |

# Appendix C: Case Studies

## Ransomware Attacks Against U.S. Agricultural Cooperatives

Multiple ransomware attacks targeted food and agriculture cooperatives during the 2021 harvest season. In September 2021, a ransomware attack struck an Iowa grain cooperative, demanding $5.9 million in cryptocurrency for a decryption tool. The grain cooperative primarily purchases grain, corn, and soybeans for processing and selling seeds and herbicides to farmers. In a statement immediately following the attack, the grain cooperative said they proactively took systems offline to contain the potential impact of the attack and disabled their soil-mapping platform to protect customers.[[12]](#footnote-13) Grain cooperative employees reverted to manual operations, writing paper tickets for cargo weights and other specifications. While this was a significantly slower process than the largely-automated system the company built, they were able to remain open and continue day to day business operations.[[13]](#footnote-14) In addition to slowing operations, the attack resulted in an exfiltration of financial information, proprietary software, and research and development data.[[14]](#footnote-15) A week after the Iowa cooperative attack, a Minnesota-based grain cooperative suffered a ransomware attack. The attack left the cooperative unable to fulfill feed orders for livestock.[[15]](#footnote-16) While the cooperative worked to return systems to normal, they relied on assistance from local cooperatives and went to manual operations, completing work by hand.

In 2022 the FBI issued a security alert to U.S., Australian, and United Kingdom based food and agricultural cooperatives, emphasizing “ransomware actors may be more likely to attack agricultural cooperatives during critical planting and harvest seasons, disrupting operations, causing financial loss and negatively impacting the food supply chain."[[16]](#footnote-17) The FBI stressed the following protective actions: backing up data, storing password protected backup copies offline, air gapping, network segmentation, and development of an operations plan in the event that systems go offline.

## Cold Storage Operations Halted by Ransomware

In April 2023, a significant cyberattack hit a major U.S. based cold storage company. The company operates temperature-controlled warehouses that food producers, distributors, and retailers use to preserve food during production, transportation, and storage.[[17]](#footnote-18) The attack primarily affected phones, online resources, and other logistical assets. The company chose to shut down its systems once the breach was discovered to prevent further damage and lateral movement to additional systems. All inbound deliveries and almost all outbound orders were cancelled for over a week.[[18]](#footnote-19)

# 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 operational script/code and proprietary research. 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>)

## Ransomware

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

### Additional Resources

* CISA Stop Ransomware Website (<https://www.cisa.gov/stopransomware>)
* CISA Stop Ransomware Guide (<https://www.cisa.gov/resources-tools/resources/stopransomware-guide>)
* Protecting Against Ransomware (<https://www.cisa.gov/news-events/news/protecting-against-ransomware>)

## 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 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 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.[[19]](#footnote-20) 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 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)

Food and Agriculture Sector Resources

* CISA Food and Agriculture Sector (<https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/food-and-agriculture-sector>)
* Food and Agriculture Information Sharing and Analysis Center (ISAC) (<https://www.it-isac.org/foodandag-isac>)

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

* Cyber Security Evaluation Tool (CSET) (<https://www.cisa.gov/downloading-and-installing-cset>)
* 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. 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 & Advisories,” <https://www.cisa.gov/news-events/cybersecurity-advisories>. [↑](#footnote-ref-4)
4. NIST Cybersecurity Framework, v2.0 (CSF 2.0) via NIST’s CPRT, “ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.AM-05>. [↑](#footnote-ref-5)
5. CISA Resources, “Zero Trust Maturity Model,” <https://www.cisa.gov/zero-trust-maturity-model>. [↑](#footnote-ref-6)
6. NIST CSF 2.0 via CPRT, “PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.DS-01>. [↑](#footnote-ref-7)
7. 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-8)
8. NIST CSF 2.0 via CPRT, “PR.PS-01: Configuration management practices are established and applied,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.PS-01>. [↑](#footnote-ref-9)
9. 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-10)
10. 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-11)
11. NIST CSF 2.0 via CPRT, “ID.IM: Improvements – Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.IM>. [↑](#footnote-ref-12)
12. David Uberti, “Iowa Grain Cooperative Hit by Cyberattack Linked to Ransomware Group,” *Wall Street Journal,* September 20, 2021, <https://www.wsj.com/articles/iowa-grain-cooperative-hit-by-cyberattack-linked-to-ransomware-group-11632172945>. [↑](#footnote-ref-13)
13. William Turton, “BlackMatter hits grain cooperative with ransomware attack,” *Farm Futures*, September 20, 2021, [https://www.farmprogress.com/business/blackmatter-hits-grain-cooperative-with-ransomware-attack](https://urldefense.us/v3/__https:/www.farmprogress.com/business/blackmatter-hits-grain-cooperative-with-ransomware-attack__;!!BClRuOV5cvtbuNI!GHAJeeKrr_eDb-CV0S-LcUove8Bdq_L_opvYOLpwdYCyVrSn1U_Im_IB1EVj3cIYBYN2ErGcaq-IBJUA8Jfi1nxgdqK8DrcMe9E$). [↑](#footnote-ref-14)
14. Uberti. [↑](#footnote-ref-15)
15. Victoria Myers, “Agricultural Cooperatives Targeted by Cyberattackers,” Progressive Farmer, April 20, 2022, <https://www.dtnpf.com/agriculture/web/ag/news/business-inputs/article/2022/04/20/agricultural-cooperatives-targeted>. [↑](#footnote-ref-16)
16. Federal Bureau of Investigation – Cyber Division, “PIN #2022420-001, “FBI Private Industry Notification: Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons,” April 20, 2022, <https://www.ic3.gov/Media/News/2022/220420-2.pdf>. [↑](#footnote-ref-17)
17. Jonathan Greig, “Cold storage company Americold reports cyberattack to SEC,” *The Record*, May 1, 2023, [https://therecord.media/cold-storage-company-americold-reports-cyberattack](https://urldefense.us/v3/__https:/therecord.media/cold-storage-company-americold-reports-cyberattack__;!!BClRuOV5cvtbuNI!GHAJeeKrr_eDb-CV0S-LcUove8Bdq_L_opvYOLpwdYCyVrSn1U_Im_IB1EVj3cIYBYN2ErGcaq-IBJUA8Jfi1nxgdqK8pKhPPTA$). [↑](#footnote-ref-18)
18. Sergiu Gatlan, “Cold storage giant Americold outage caused by network breach,” *Bleeping Computer*, April 28, 2023, [https://www.bleepingcomputer.com/news/security/cold-storage-giant-americold-outage-caused-by-network-breach/](https://urldefense.us/v3/__https:/www.bleepingcomputer.com/news/security/cold-storage-giant-americold-outage-caused-by-network-breach/__;!!BClRuOV5cvtbuNI!GHAJeeKrr_eDb-CV0S-LcUove8Bdq_L_opvYOLpwdYCyVrSn1U_Im_IB1EVj3cIYBYN2ErGcaq-IBJUA8Jfi1nxgdqK89PHKgMI$). [↑](#footnote-ref-19)
19. 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-20)