

**CISA Tabletop Exercise Package**

**Commercial Facilities**

## [Enter Organization Name]

## <Insert Date>

Updated November 2023

## Cybersecurity and Infrastructure Security Agency

Table of Contents

[Handling Instructions 3](#_Toc143606182)

[Exercise Overview 5](#_Toc143606188)

[General Information 6](#_Toc143606189)

[Module 1 8](#_Toc143606190)

[Module 2 10](#_Toc143606191)

[Appendix A: Additional Discussion Questions 12](#_Toc143606192)

[Appendix B: Acronyms 15](#_Toc143606193)

[Appendix C: Case Studies 16](#_Toc143606194)

[Appendix D: Malicious Activity 18](#_Toc143606195)

[Appendix E: Contacts and Resources 19](#_Toc143606196)

# 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 | Assess <Commercial Facility>’s cyber resilience and ability to respond to a significant a cyber incident during a special event. | |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Govern, Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Assess organizational cyber resilience before, during, and following a cyber incident impacting a special event. 2. Examine incident response plans, policies, and capabilities. 3. Discuss the procedures for cyber incident information sharing and coordination. | |
| Threat or Hazard | Cyber Incident – Phishing, Ransomware | |
| Scenario | * Commercial facility event staff receive a phishing email asking for login credentials. * Event ticket buyers also receive an email with a malicious link. * During a special event, a commercial facility is a victim of a ransomware attack. * The cyber incident garners media attention. | |
| Sponsor | Exercise Sponsor | |
| Participating Organizations | Overview of organizations participating in the exercise (e.g., federal, state, local, private sector, etc.). | |
| Points of Contact | |  |  | | --- | --- | | **Insert Organization POC(s)**  Contact Information | **CISA National Cyber Exercise Program (NCEP)**  [cisa.exercises@cisa.dhs.gov](mailto:cisa.exercises@cisa.dhs.gov) | | |

# General Information

## Building Resilience

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

## Using this Situation Manual

Modules 1 and 2 contain the scenario injects and discussion questions you will use to conduct the exercise. There are footnotes with corresponding resources throughout the modules to guide your preparedness efforts. The appendices provide the following information to tailor the exercise discussion:

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

## Participant Roles and Responsibilities

**Players** have an active role in discussing or performing their primary roles and responsibilities during the exercise. Players discuss or initiate actions in response to the scenario. Players may include IT/information security staff, physical security staff, and emergency management staff.

**Observers** do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise. Observers may include senior-level staff such as management/leadership.

**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 possible phishing attempt targeting both event staff and customers.
  + **Module 2:** This module introduces customer services issues and a ransomware attack at the start of the special event.
* Hotwash
* ***Structure Note:*** *Modules, timeline dates, and discussion questions included in each module may be modified as desired. Additional discussion questions for each module can be found in Appendix A.*

## Exercise Guidelines

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

## Exercise Hotwash and Evaluation

The facilitator will lead a hotwash with participants at the end of the exercise to address any ideas or issues that emerge from the exercise discussions.

# Module 1

### 4 Months Before the Special Event

The Cybersecurity & Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) release a joint advisory warning a sophisticated ransomware group is targeting events of all sizes within the commercial facilities sector.[[2]](#footnote-3) The advisory notes tactics, techniques, and procedures (TTPs) used by the group includes both direct social engineering attacks against the host organizations as well as the third party ticketing/Point of Sale (POS) vendors. Two days after the advisory is released, national news reports a high-profile professional sports team is the victim of a ransomware attack just days before the championship game.

## 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 cyber threats to your organization?
2. What cybersecurity threat information does your organization receive?
   1. What cyber threat information is most useful?
   2. How is information disseminated to relevant parties within your organization?
   3. What actions would your organization take in response to an alert like the one presented in the scenario?

### 3 Months Before the Special Event

Several employees at <commercial facility> receive an email asking them to verify their account credentials, including usernames, passwords, and personal security question answers.[[3]](#footnote-4) Many employees report the email as suspicious; however, some click the link and complete the form.[[4]](#footnote-5)

1. Describe your organization’s cybersecurity training program for employees.
   1. How often are employees required to complete this training?
   2. What additional training is required for employees who have system administrator-level privileges?
   3. If event volunteers have network access, what cybersecurity training do they receive?
   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?

### 2 Months Before the Special Event

Fans who purchased tickets for the upcoming event receive a survey email from the ticket vendor asking questions regarding overall satisfaction and buying experience. When they click the link, it leads to a blank website. Many customers report the faulty link to the ticketing vendor.

After an investigation, the ticketing vendor reports they have no record of sending a survey email to customers.

### 6 Weeks Before the Special Event

The <commercial facility> IT department conducts system scans on critical event technology and discovers unpatched vulnerabilities, including uninstalled patches available for the past 3 months for your <ticketing/reservations/merchandise/POS system>. Security patches are applied.

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. Describe your organization’s asset management plan and how you prioritize critical assets.
   3. Does your organization have a vulnerability management program dedicated to mitigating known exploited vulnerabilities in internet-facing systems?
2. Describe your patch and vulnerability management plan.
3. What risk assessments are performed on network servers?
4. What processes are in place to proactively evaluate each server’s criticality and applicability to software patches?
5. What considerations are addressed in the plan’s risk management strategy (e.g., extended downtime, loss of data, impaired functionality)?
6. What is the role of cybersecurity in the review and selection of third-party vendor support?[[5]](#footnote-6)
   1. What cybersecurity language (e.g., cybersecurity training and cyber incident notification requirements) is included within third-party vendor contracts?
   2. How do you evaluate the cybersecurity posture of your vendors?
   3. How often are contracts reviewed?
7. What level of access do your third-party vendors have to your organization’s network?[[6]](#footnote-7)
   1. What mechanisms or processes are in place to prevent malicious activity?
   2. How often are third-party access rights and data logs reviewed?

### 3 Weeks Before the Special Event

Customers call your help line to report difficulties purchasing <tickets/reservations/merchandise>. This is the same system your IT department patched 3 weeks ago.

1. How would your organization address issues with the <ticketing/reservation/merchandise> system?

# Module 2 – Day of the Special Event

### 10:45 a.m.

Guests arriving to the venue report issues with the ticketing application (app). Some are unable to access their tickets, while others report buffering in the app. Lines develop at multiple entrances around the venue. Guests with printed tickets have no issues with entry.

Discussion Questions

1. What alternate processes do you have to manage event ticketing if your primary ticketing system malfunctions?
   1. Does the size of the crowd change your response?
2. What role do third-party vendors play within your organization’s incident response plan?

### 12:30 p.m.

Prior to the event, concession and merchandise staff report to managers that the Point of Sale (POS) system is functioning slowly. As staff work to find a solution, the POS system shuts down entirely.

1. What are the impacts of the loss of the POS system to your organization?
   1. How would you address the loss of the POS system?

### 2:00 p.m.

A ransom note appears on multiple computer screens visible to guests throughout the venue. The message states that the event was hacked, and files from the venue and personal fan information were stolen and encrypted. The ransom note demands a payment of <insert ransom amount (e.g., $250,000)> within 24 hours, or the attacker will sell the data.

1. Using your organization’s cyber incident response plan (CIRP), describe the actions your organization would take to minimize impact to the event and operations.
   1. How can you use manual and alternative systems to maintain operations?
   2. How are IT and business continuity functions coordinated with physical security?
2. Explain your organization’s decision-making process regarding ransomware payment.[[7]](#footnote-8)
   1. Are ransomware policies/procedures included in your CIRP?
   2. How are your cyber insurance provider or third-party vendors involved in your procedures?
   3. Discuss potential legal and reputational ramifications of paying or not paying the ransom.
3. What factors are considered when deciding to cancel an event?
   1. Who makes the decision?
   2. Would this scenario result in the shutdown of an event?

### 6:00 p.m.

Later that day, local news stations run stories on the ransomware attack featuring interviews with angry and concerned guests. Your organization receives requests for comments on the situation.

1. How sufficient are your organization’s current internal resources for responding to the cyber incidents in this scenario?[[8]](#footnote-9)
2. What additional resources outside of your organization are 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, incident response vendors) would you contact for assistance?
5. What information are you sharing internally?
6. Describe your organizational processes to respond to the media reports and inquiries.[[9]](#footnote-10)
7. What pre-scripted messages have been developed for cyber incidents?
8. How would public messaging be coordinated and disseminated during a cyber incident?
9. How would you preserve and reinforce the public’s confidence and trust in your organization during a significant cyber incident?
10. What legal and regulatory notifications are required based on the scenario?
    1. When are notifications  made and who is responsible for making the notifications?
11. Based on discussion, what changes will you implement to increase the resilience of your organization?

# Appendix A: Additional Discussion Questions

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

## Cyber Resilience

1. Discuss how cyber preparedness is integrated into your current all-hazards preparedness efforts.
2. How often are your cybersecurity plans, policies, and procedures externally reviewed or audited?
   1. What were the most recent results and action items that followed?
3. Describe your organization’s review process for your CIRP.
4. How often is the CIRP reviewed?
5. Which individual(s) and department(s) are responsible for reviewing and updating the plan?
6. How are updates to the plan communicated to relevant employees?
7. Discuss your supply chain concerns related to cybersecurity infrastructure.
8. What is your method for tracking and identifying firmware vulnerabilities in your network?
9. 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?
10. How is the integrity of your critical data protected and validated?
11. What external entities have access to the database?
12. How do those entities report a compromise of their systems to your office?
13. How does your organization maintain availability of key assets (e.g., network connectivity, etc.)?
14. If primary communications are compromised, how do you provide information to internal and external entities?
15. What policies and procedures does your organization use to decide when and how to restore backed-up data?
    1. How does your organization incorporate measures for ensuring the integrity of backup data before restoration?

## Accounts & Privileges

1. Describe your organization’s employee off-boarding process.
2. Is this process coordinated with IT and HR?
3. What additional actions are taken if the employee’s termination is contentious?
4. 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?
5. What are your organization’s policies or procedures for IT account management?
6. What are the protocols for establishing, activating, modifying, disabling, and removing accounts?

## Incident Identification

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

## Incident Response

1. What are your processes for collecting evidence and maintaining the chain of custody during a cyber incident?
2. At what point in the scenario would you contact law enforcement?
3. How would a law enforcement investigation impact containment, eradication, and recovery efforts?
4. How would a compromise of vendor(s) affect your organization if they have access to your information?
5. What are the notification requirements to your organization for incidents?
6. What are the processes for contacting critical personnel outside of core hours?
7. How do you proceed if critical personnel are unreachable or unavailable?
8. Who is responsible for coordinating information across different organizational-level 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 re-activating critical business processes and systems?
6. How long and costly is the process to completely rebuild these systems?
7. What factors do you consider when making these decisions?

## Training & Exercises

1. What training does your cybersecurity incident response team undergo to detect, analyze, and report malicious activity?
   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 Emergency Operations Center/Security 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. What training is provided to employees regarding reporting contact with the media?
      2. How do you build and maintain trust with your customers?

## Legal

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

# Appendix B: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| CIRP | Cyber Incident Response Plan |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CPG | Cybersecurity Performance Goals |
| CSF | Cybersecurity Function |
| DHS | U.S. Department of Homeland Security |
| FBI | Federal Bureau of Investigation |
| IT | Information Technology |
| NCEP | Nation Cyber Exercise Program |
| NIST | National Institute of Standards and Technology |
| PII | Personally Identifiable Information |
| POS | Point of Sale |
| TLP | Traffic Light Protocol |
| TTPs | Tactics, Techniques, and Procedures |

# Appendix C: Case Studies

Ransomware Attacks Against Gambling and Entertainment Companies

On September 7, 2023, a major U.S. based gambling and entertainment company was breached by a well-known ransomware group. The attackers gained access by using social engineering on a third-party IT vendor hired by the entertainment company.[[10]](#footnote-11) Once the malicious actors infiltrated the system, they were able to steal a copy of the loyalty program database, giving them access to customer Personally Identifiable Information (PII) such as Social Security numbers and driver’s license numbers. The company made half of the ransom payment, totaling $30 million, to avoid the stolen data from being distributed to unknown parties.[[11]](#footnote-12) The company stated that it had taken every measure possible to get the hacker group to delete stolen PII; however, they have no way of knowing if it was deleted.

A similar attack by the same ransomware group against a different major gambling and entertainment company caused the shutdown of on-site ATMs and slot machines, costing them an estimated $100 million in losses and $10 million in one-time expenses.[[12]](#footnote-13)

## Ransomware Attack Against Professional Football Team

On February 11, 2022, the FBI and Secret Service released an advisory to inform critical infrastructure organizations of a recent increase in the deployment of a specific ransomware variant used by a sophisticated ransomware group. Three days later, a professional American football team was targeted by the same group. The ransomware group is known to target Western governments and cultural organizations.[[13]](#footnote-14) After an investigation, the team’s corporate IT network seemed to be the only systems affected by the incident. Systems designed to handle ticket holders and stadium operations stayed intact and unaffected. The football team hired a third-party cybersecurity vendor to help mitigate and recover from the incident. Additionally, the team notified law enforcement who assisted with the investigation. The incident occurred days before the Super Bowl.

## Multinational Retail Company Data Breach

A leading multinational retail store specializing in affordable fashion was hit by a cyber incident in early 2023. The threat actors gained access to the company’s network between early January and late March of 2023. The threat actors targeted the company’s employee database, stealing PII of over 500,000 current and former employees.[[14]](#footnote-15) Stolen information included full names, Social Security numbers, dates of birth, bank account information, and health insurance plan information. Customer data was not breached.

While not admitting to paying a ransom, the company did report that they acted, resulting in the hackers erasing stolen data along with any evidence of communication between the threat actors and the company. No ransomware group came forward claiming responsibility for the incident, and both parties deleted evidence of communications.[[15]](#footnote-16)

# Appendix D: Malicious Activity

## 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: 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 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 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/>)

Commercial Facilities Sector Resources

* Commercial Facilities Sector Resources: (<https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/commercial-facilities-sector#:~:text=The%20Commercial%20Facilities%20Sector%20includes,business%2C%20entertainment%2C%20or%20lodging.>)
* Media and Entertainment Information Sharing and Analysis Center (<https://www.meisac.org/>)
* Real Estate Information Sharing and Analysis Center (<https://www.reisac.org/>)

Private Sector/Business Resources

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

Preparedness Resources

* CISA Cross-sector Cybersecurity Performance Goals (<https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist>)
* 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. NIST Cybersecurity Framework, v2.0 (CSF 2.0) via NIST’s CPRT, “ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.RA-02>. [↑](#footnote-ref-3)
3. NIST 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-4)
4. NIST CSF 2.0 via CPRT, “PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.AT-01>. [↑](#footnote-ref-5)
5. NIST CSF 2.0 via CPRT, “GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=GV.SC-05>. [↑](#footnote-ref-6)
6. NIST CSF 2.0 via CPRT, “PR.AA: Identity Management, Authentication, and Access Control,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.AA>. [↑](#footnote-ref-7)
7. CISA, “Stop Ransomware,” <https://www.cisa.gov/stopransomware> [↑](#footnote-ref-8)
8. NIST CSF 2.0 via CPRT, “GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=GV.RR-01>. [↑](#footnote-ref-9)
9. NIST CSF 2.0 via CPRT, “RC.CO-04: Public updates on incident recovery are shared using approved methods and messaging,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RC.CO-04>. [↑](#footnote-ref-10)
10. [Zeba](https://www.reuters.com/business/casino-giant-caesars-confirms-data-breach-2023-09-14/) Siddiqui, “Hackers say they stole 6 terabytes of data from casino giants MGM, Caesars” *Reuters*, September 14, 2023, <https://www.reuters.com/business/casino-giant-caesars-confirms-data-breach-2023-09-14/>. [↑](#footnote-ref-11)
11. Zach Whittaker “[Caesars Entertainment says customer data stolen in cyberattack” *TechCrunch*](https://techcrunch.com/2023/09/14/caesars-entertainment-data-breach-cyberattack/), September 14, 2023, <https://techcrunch.com/2023/09/14/caesars-entertainment-data-breach-cyberattack/>. [↑](#footnote-ref-12)
12. Carly Page, “[MGM Resorts confirms hackers stole customers’ personal data during cyberattack” *TechCrunch*](https://techcrunch.com/2023/10/06/mgm-resorts-admits-hackers-stole-customers-personal-data-cyberattack/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuYmluZy5jb20v&guce_referrer_sig=AQAAALFxT8K4lNPYJLNDYeHvH7iHM7FM1I_fkF_6-iFSl4iJuF4hYu-b6DxB0-ACCQcANb4yzwrNJi9wh-vpc7CSdoqJKuOXN9LDG-rj57aeywiGu2XgxiC-3K6Ve43c1hts0CCJvZkW7drTuXnhddoGl_0M9jdMGly-jQdU_S31k6D2), October 6, 2023, [https://techcrunch.com/2023/10/06/mgm-resorts-admits-hackers-stole-customers-personal-data-cyberattack/?guccounter=1&guce\_referrer=aHR0cHM6Ly93d3cuYmluZy5jb20v&guce\_referrer\_sig=AQAAALFxT8K4lNPYJLNDYeHvH7iHM7FM1I\_fkF\_6-iFSl4iJuF4hYu-b6DxB0-ACCQcANb4yzwrNJi9wh-vpc7CSdoqJKuOXN9LDG-rj57aeywiGu2XgxiC-3K6Ve43c1hts0CCJvZkW7drTuXnhddoGl\_0M9jdMGly-jQdU\_S31k6D2](https://techcrunch.com/2023/10/06/mgm-resorts-admits-hackers-stole-customers-personal-data-cyberattack/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuYmluZy5jb20v&guce_referrer_sig=AQAAALFxT8K4lNPYJLNDYeHvH7iHM7FM1I_fkF_6-iFSl4iJuF4hYu-b6DxB0-ACCQcANb4yzwrNJi9wh-vpc7CSdoqJKuOXN9LDG-rj57aeywiGu2XgxiC-3K6Ve43c1hts0CCJvZkW7drTuXnhddoGl_0M9jdMGly-jQdU_S31k6D2.). [↑](#footnote-ref-13)
13. Sean Lyngaas “[San Francisco 49ers confirm network security incident” *CNN*](https://www.cnn.com/2022/02/13/us/49ers-network-security-incident/index.html), February 13, 2022, <https://www.cnn.com/2022/02/13/us/49ers-network-security-incident/index.html>. [↑](#footnote-ref-14)
14. Jurgita Lapiente, “[Forever 21 discloses data breach: 500K+ affected” *Cybernews*](https://cybernews.com/news/forever-21-data-breach/), August 30, 2023, <https://cybernews.com/news/forever-21-data-breach/>. [↑](#footnote-ref-15)
15. B. Toulas, “[Forever 21 data breach: hackers accessed info of 500,000” *BleepingComputer*](https://www.bleepingcomputer.com/news/security/forever-21-data-breach-hackers-accessed-info-of-500-000/), August 31, 2023, <https://www.bleepingcomputer.com/news/security/forever-21-data-breach-hackers-accessed-info-of-500-000/>. [↑](#footnote-ref-16)